UNIVERSITY OF TORONTO
3 1761 01018579 1

QA
247
B7
pt.1

NON-COMMUTATIVE RINGS

(Part I)

by

RICHARD BRAUER

E. WEISS

HARVARD UNIVERSITY
CAMBRIDGE, MASSACHUSETTS

NON-COMMUTATIVE RINGS

(Part I)

by

Richard Brauer

E. Weiss

HARVARD UNIVERSITY
Cambridge, Massachusetts

QA
247
B7
pt.1

LIBRARY
NOV 21 1967
UNIVERSITY OF TORONTO

Chapter I

DEFINITION OF RINGS AND ALGEBRAS. EXAMPLES.

In this chapter, we are concerned with the definition of rings and algebras. We then give a number of illustrations which will be useful and instructive later.

1. Definition of a ring. First properties.

We consider a set R for which an addition and a multiplication are defined within R. This is to say that two functions $s(x,y)$ and $p(x,y)$ of two arguments $x,y \in R$ have been selected, both with values in R. We write $x+y$ for $s(x,y)$ and xy for $p(x,y)$.

DEFINITION 1. A set R for which an addition and a multiplication are defined in R is a ring, if

(I) The elements of R form an abelian group under addition.

(II) The multiplication is associative: $(ab)c = a(bc)$ for arbitrary $a, b, c \in R$.

(III) Both distributive laws hold:

$$a(b+c) = ab + ac, \qquad (b+c)a = ba + ca$$

for arbitrary a, b, c in R.

As a consequence of (I), we note that for given $a, b \in R$ the equation $a+x=b$ has a unique solution $x \in R$ which is denoted by $x=b-a$. For $a \in R$, the element $a-a$ is independent of a and is called the zero-element 0 of R. Then $b+0=b$ for any $b \in R$. As usual, we write $-a$ for $0-a$. Then $b-a=b+(-a)$. It follows from the associativity of the addition that, for any positive integer n, we can form sums of n elements of R without using parentheses. In particular, we write na for a sum of n equal terms $a \in R$.

Similarly, because of (II), we can form products of n elements of R without using parentheses. The product of n equal factors a is of course denoted by a^n.

Taking $b=c=0$ in (III), we see that $a0=0$, $0a=0$ for every $a \in R$. It then follows from (III) for $c=-b$, $b \in R$, that $a(-b)=-ab$, $(-b)a=-ba$. The ordinary rules for brackets hold. However, since the commutativity of multiplication was not assumed, we have to be careful about the order of the factors. A ring is said to be commutative, if $ab=ba$ for all $a, b \in R$.

Let R be a ring which does not only consist of the single element 0. It may happen that there exists an element e in R such that $ea=ae=a$ for all $a \in R$. Then $e \neq 0$ and further e is uniquely determined. We call e the unit element of R and often denote it by 1. If R is a ring with a unit element 1, an element a of R is said to be regular, if there exists an element a' of R such that $aa'=a'a=1$. Then a' is uniquely determined by a. We usually write a^{-1} for a and call a^{-1} the inverse of a.

DEFINITION 2. A skew field is a ring R with unit element such that every element $a \neq 0$ has an inverse. Alternately, we may say that the ring R is a skew field, iff the elements different from 0 form a group under multiplication. A field is a commutative skew field.

Before we come to the discussion of examples, it should be mentioned that, as in all abstract theories, we are not interested in what the elements of R "are" but only how they "behave" under addition and multiplication. This leads to the idea of isomorphism.

DEFINITION 3. An isomorphism of a ring R onto a ring R^* is a one-to-one mapping $x \longrightarrow x^*$ of R onto R^* such that $(x+y)^* = x^*+y^*$, $(xy)^* = x^*y^*$ for all $x, y \in R$. The rings R and R^* are isomorphic, in symbols $R \approx R^*$, if isomorphisms of R onto R^* exist.

If we have an isomorphism of R onto R^* and if we agree to use the same letter for an element x of R and the corresponding element of R^*, then any equation based on the ring properties in R is true in R^* and vice versa. In a way, we may say that R and R^* differ "in name only" or that the rings R and R^* are "not essentially different". We cannot distinguish between them in an intrinsic manner using only ring properties. It will be clear that an isomorphism of R onto R^* maps the zero-element of R on that of R^*, the unit element of R (if it exists) on the unit element of R^*, etc. We have $(x-y)^* = x^*-y^*$ for $x, y \in R$.

2. Rings of endomorphisms of abelian groups.

We discuss a special class of rings which will be of fundamental importance.

Let G be an abelian group in which the group operation is written as addition. Consider first the set M of all mappings θ of G into G. Such mapping is given, if for every $g \in G$, the element is known on which g is mapped. We denote this image by $g\theta$ or by $\theta(g)$. Of course, the notion of a mapping is the same as that of a function defined on G with values in G. Two mappings θ and $\theta' \in M$ are equal, iff $g\theta = g\theta'$ for all $g \in G$.

The sum of two elements θ_1, θ_2 of M is defined by the formula

$$(1) \qquad g(\theta_1 + \theta_2) = g\theta_1 + g\theta_2 \qquad \text{(for all } g \in G).$$

Here the element on the right makes sense, since $g\theta_1$, $g\theta_2 \in G$, and G is an additive group. In other words, $\theta_1+\theta_2$ is the mapping which maps the element $g \in G$ on the sum of its images $g\theta_1$, $g\theta_2$ for the two mappings θ_1, θ_2. This is the usual definition of the sum of two functions. It will be clear from this that M itself is an abelian group under addition. The zero-element is the zero-mapping $\Box$ of G which maps every $g \in G$ on the zero-element 0 of G;

$$g\Box = 0 \qquad (\text{for all } g \in G). \tag{2}$$

If $\theta \in M$, the mapping $-\theta$ is given by

$$g(-\theta) = -(g\theta). \tag{3}$$

Here, the element $-(g\theta)$ is the negative of the element $g\theta$ of the additive group G.

We next define the product of two transformations $\theta_1, \theta_2 \in M$ by the formula

$$g(\theta_1\theta_2) = (g\theta_1)\theta_2 \qquad (\text{for } g \in G). \tag{4}$$

Thus, $\theta_1\theta_2$ is the mapping obtained by performing θ_1 first which maps $g \rightarrow g\theta_1$ and following it up by θ_2 which takes $g\theta_1 \rightarrow (g\theta_1)\theta_2$. It is seen at once that this multiplication is associative. Moreover, if $\theta, \theta_1, \theta_2$ are three elements of M and if $\sigma_1 = \theta(\theta_1+\theta_2)$ and $\sigma_2 = \theta\theta_1+\theta\theta_2$, it follows from the definitions of addition and multiplication of mappings that both σ_1 and σ_2 map $g \rightarrow (g\theta)\theta_1 + (g\theta)\theta_2$. Hence $\sigma_1 = \sigma_2$, i.e., we have the left distributive law

$$\theta(\theta_1+\theta_2) = \theta\theta_1 + \theta\theta_2.$$

However, M is not a ring, since the right distributive law is not true in general.

In order to obtain a ring, we replace M by the subset E consisting of the endomorphisms of G. An endomorphism θ of G is simply a homomorphic mapping of G into G, i.e., a mapping of G into G such that

$$(5) \qquad (g_1+g_2)\theta = g_1\theta+g_2\theta \quad ,$$

for all g_1, $g_2 \in G$.

If we apply θ to both sides of (1) and use (5) for $g_1=g\theta_1$, $g_2=g\theta_2$, we see that $g((\theta_1+\theta_2)\theta) = g(\theta_1\theta)+g(\theta_2\theta) = g(\theta_1\theta+\theta_2\theta)$ for all $g \in G$ and hence we have the right distributive law

$$(\theta_1+\theta_2)\theta = \theta_1\theta+\theta_2\theta$$

for θ_1, $\theta_2 \in M$ and $\theta \in E$. In order to see that E is a ring, it is necessary to check that if θ_1, θ_2 are in E, then $\theta_1 \pm \theta_2$, $\theta_1\theta_2$ lie in E. This is done easily. Note though that the proof of $\theta_1 \pm \theta_2 \in E$ depends on the commutativity of G. Note also that $\square \in E$ so that E is not empty. Actually, the identical mapping I of G,

$$(6) \qquad gI = g \qquad \text{for all } g \in G ,$$

is an endomorphism and clearly, I is the unit element of E. We have thus shown

THEOREM (A). The endomorphisms of an abelian group G form a ring E with unit element I.

Remarks. 1. An element $\theta \in E$ has a reciprocal, iff θ is an automorphism, i.e., an isomorphism of G onto G. Indeed, if θ is such an isomorphism, the reciprocal mapping θ^{-1} is an isomorphism of G onto G too and $\theta\theta^{-1} = \theta^{-1}\theta = I$. Conversely, if we have two elements θ, θ' of E such that $\theta\theta' = I$ then θ must be one-to-one, since otherwise $\theta\theta' = I$ could not be one-to-one. Further, if $\theta'\theta = I$ then θ must map G onto G, since otherwise $\theta'\theta = I$ could not map G onto G. Hence θ has a reciprocal, only if it is an isomorphism of G onto G.

2. Our theorem remains true, if G is an abelian operator-group with a set K of operators, if by an endomorphism θ we now mean an operator-homomorphism of G into G. Actually, the ring of endomorphisms in this sense is a "subring" of the ring E obtained when we forget about the operators. (Cf. the Appendix for the definition of an operator group.)

3. Suppose that G is a simple abelian group, i.e., that (0) and G itself are the only subgroups of G. Since any $\theta \in E$ maps G on a subgroup $G\theta$ of G, we have either $g\theta = (0)$ or $G\theta = G$. In the first case, $\theta = \square$. Thus, if $\theta \neq \square$, θ maps G onto G. Again, the kernel N of the homomorphism θ is a subgroup of G and hence either $N = G$ or $N = (0)$. In the former case, $\theta = \square$; in the latter case, θ is an isomorphism. Hence any $\theta \neq \square$ in E is an automorphism of G. The Remark 1 then shows that E is a skew field, since any $\theta \neq \square$ has a reciprocal θ^{-1}.

If we consider groups without operators, the significance of this remark is very limited, since the only simple abelian groups are the cyclic groups of prime order (discussed in the following section). However, our remark applies also to operator groups G. Here, simplicity means that (0) and G are the only admissible subgroups. Since there exist many simple operator-groups, we can obtain many skew fields in this manner.

4. If we use the "functional" notation $\theta(g)$ instead of $g\theta$ for the image of g, it is customary to write $\theta_2 \circ \theta_1$ (with this order of the factors) for our $\theta_1\theta_2$. Then the formula (4) takes the form

$$(\theta_2 \circ \theta_1)(g) = \theta_2(\theta_1(g)). \tag{4*}$$

3. Special cases.

We discuss briefly some special cases of rings of endomorphisms.

Take first the case of a cyclic group $G = \{\sigma\}$. An endomorphism θ of G maps the generating element σ of G on some element $n\sigma$ of G, n a rational integer. If θ maps $\sigma \to n\sigma$, it follows that $r\sigma \to rn\sigma$ for any rational integer r. Hence, θ is completely determined by the number n and we denote now θ by the symbol $[n]$. Conversely, for any fixed n, the mapping $r\sigma \to rn\sigma$, $(r=0, \pm 1, \pm 2, \ldots)$ is an endomorphism of G. Thus, E consists of the elements $[n]$, $(n=0, \pm 1, \pm 2, \ldots)$; $[n] : r\sigma \to rn\sigma$ for $r = 0, \pm 1, \pm 2, \ldots$. The mappings $[n]$ need not all be distinct. Indeed, we have $[n] = [n']$ iff $n\sigma = n'\sigma$. If G is cyclic of finite order m, then this is so, iff $n \equiv n' \pmod{m}$. On the other hand, if G has infinite order, then $n\sigma = n'\sigma$ means $n = n'$. If we set $m = 0$ in this case, we have

$$[n] = [n'] \Longleftrightarrow n \equiv n' \pmod{m} .$$

For two integers n_1 and n_2, we see at once from (1) that $[n_1] + [n_2]$ maps $\sigma \to (n_1+n_2)\sigma$ and from (4) that $[n_1][n_2]$ maps $\sigma \to n_1 n_2 \sigma$. Hence

$$[n_1] + [n_2] = [n_1+n_2] , \qquad [n_1][n_2] = [n_1 n_2] .$$

Thus, in the case of an infinite cyclic group, the ring E is isomorphic with the ring Z of rational integers. In the case of a cyclic group of finite order m, the ring E is the ring of integers (mod m). In particular, if m is a prime number p, then E is a skew field (§2, remark 3) and since it is commutative, it is a field.

As our next example, let K be a given field and let G be a vector space over K. Then G is an additive abelian group with K as domain of operators. If we consider G as a K-group, (§2, remark 2), the endomorphisms are exactly the linear transformations of G into G. Thus, E is the ring of linear transformations θ of G. Each θ can be described by a matrix (see the Appendix) and E is isomorphic with a ring of matrices.

4. Rings of functions.

We discuss another type of ring which arises in a natural manner. Let S be an arbitrary set of elements and let R be a given ring. The set F of all functions defined in S with values in R forms a ring, if the sum and the product of functions both are defined in the usual manner. Thus, if $f, g \in F$, then $f+g$ and fg are the functions defined by $(f+g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)\, g(x)$ for $x \in S$.

Consider the case that R is the ring of integers (mod 2). This ring which is obtained by taking $m = 2$ in § 3 consists of two elements 0 and 1 , and

$$0 + 0 = 0, \qquad 0 + 1 = 1 + 0 = 1, \qquad 1 + 1 = 0$$

$$0 \cdot \; 0 = 0 \qquad 1 = 1 \qquad 0 = 0, \quad 1 \qquad 1 = 1 .$$

Each function $f \in F$ is completely determined by the subset T_f of S on which f has the value 1. Conversely, to every subset T of S , we can form the characteristic function f of T which has the value 1 on T and the value 0 on the complement of T . Then $T = T_f$. In this manner, we obtain a one-to-one correspondence between the set F of all functions f and the set X of all subsets T of S (including S and the empty set $\emptyset$). Since F is a ring, we can use this one-to-one correspondence to turn X into a ring by adding and multiplying sets T in such a manner that the correspondence becomes an isomorphism. In terms of unions, intersections, and differences of sets, we have then

$$T_1 + T_2 = (T_1 \cup T_2) - (T_1 \cap T_2); \quad T_1 T_2 = T_1 \cap T_2$$

for $T_1, T_2 \in X$. This ring X is called the Boolean ring of the subsets of the given set S.

5. The notion of an algebra.

An important type of ring is given by the algebras over a field K . First, we consider more generally non-associative algebras (or, rather, "not necessarily associative" algebras).

DEFINITION 4. A non associative algebra A over a given field K is a system of elements such that

(I) A is a vector space over K .

(II) The product $\alpha\beta$ of two elements α, β of A is defined as an element of A and both distributive laws hold.

(III) The equation $c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta)$ holds for all $\alpha, \beta \in A$ and all $c \in K$.

If the associative law of multiplication holds, then A is an associative algebra. In this case, A is of course a ring.

As a vector space over K , the algebra A possesses a basis $\{\eta_i\}$ where the subscript i ranges over a certain set J of indices. The cardinal number of J , which is uniquely determined by A , is called the dimension of A and denoted by dim A = [A:K] . For us, the most important case is that dim A is finite, dim A = n .

An arbitrary element α of A has a representation

$$\alpha = \sum_{i \in J} a_i \eta_i \qquad \text{with } a_i \in K , \tag{7}$$

where only a finite number of a_i are different from 0 . These coordinates a_i of α are uniquely determined by α .

The product $\eta_i \eta_j$ of two basis elements must have a representation (7), say

$$\eta_i \eta_j = \sum_{k \in J} c_{ijk} \eta_k , \qquad (c_{ijk} \in K) , \tag{8}$$

where for given i, $j \in J$, only a finite number of c_{ijk} are different from 0. These c_{ijk} are termed the scalars of multiplication of A. They depend not only on A but also on the basis $\{\eta_i\}$.

If $\beta = \sum b_i \eta_i$ is a further element of A with the coordinates $\{b_i\}$, it follows from (II) and (III) in Definition 4 that

$$(9) \quad \alpha\beta = \sum_i a_i \eta_i \sum_j b_j \eta_j = \sum_k \Big(\sum_{i,j} a_i b_j c_{ijk}\Big) \eta_k ,$$

where all subscripts range over J. Thus, the multiplication in A is uniquely determined by the system $\{c_{ijk}\}$.

Conversely, we can start from an arbitrary vector space A over the given field K with a basis $\{\eta_i\}$, $i \in J$, and choose an arbitrary system $\{c_{ijk}\}$, i, j, $k \in J$, of elements of K such that for given i, j only a finite number of c_{ijk} are different from 0. Then multiplication in A can be defined by (9). It is obvious that A is an algebra over K. Since (8) is a special case of (9), (obtained by taking $a_i = 1$, $b_j = 1$ and all other a's and b's as zero), the c_{ijk} are the scalars of multiplication of A.

It is easy to see how the c_{ijk} change, if another basis $\{\zeta_i\}$, $i \in J^*$, is taken. We then have formulas

$$(10) \qquad \zeta_i = \sum_j p_{ij} \eta_j , \quad \eta_i = \sum_j q_{ij} \zeta_j ,$$

where the two matrices (p_{ij}) and (q_{ij}) have coefficients in K, are row finite (i.e., for given i, only a finite number of p_{ij} and q_{ij} are different from 0), and are inverse to each other. Then, it follows from (10) and (9) that

$$\zeta_r \zeta_s = \sum_k \Big(\sum_{i,j} p_{ri} p_{sj} c_{ijk}\Big) \eta_k = \sum_t \Big(\sum_{i,j,k} p_{ri} p_{sj} c_{ijk} q_{kt}\Big) \zeta_t .$$

Thus the new scalars of multiplication are

$$c'_{rst} = \sum_{i,j,k} p_{ri} p_{sj} q_{kt} c_{ijk} .$$

(The tensor specialist may notice that c_{ijk} behaves as a tensor under basis transformation (10) with i and j as cogredient indices and k as contragredient index.)

In general, the algebra A defined by choosing a vector space with a basis $\{\eta_i\}$ and picking a system $\{c_{ijk}\}$ of elements of K as scalars of multiplication will be non-associative. In order that A be associative, it will be necessary that we have

$$(11) \qquad (\eta_i \eta_j)\eta_k = \eta_i(\eta_j \eta_k) \qquad \text{for all } i,j,k \in J .$$

Conversely, if we multiply (11) with the coordinates a_i, b_j, c_k of three elements α, β, γ of A and add over all i, j, k, we obtain $(\alpha\beta)\gamma = \alpha(\beta\gamma)$. Hence (11) is necessary and sufficient for the associativity of A .

If we express the products in (11) by using (8), (9), we see easily that each equation (11) is equivalent with a quadratic equation for the scalars of multiplication

$$\sum_r c_{ijr} c_{rk\ell} = \sum_r c_{ir\ell} c_{jkr} \qquad \text{for all } i, j, k, \ell .$$

From now on, the word algebra will be reserved for associative algebras.

By an isomorphism θ of an algebra A onto an algebra A*, we mean an isomorphism $\alpha \rightarrow \alpha^*$ of the ring A onto the ring A* such that $c\alpha \rightarrow c\alpha^*$ for all $c \in K$ and all $\alpha \in A$.

6. Examples of algebras.

(a) If L is an extension field of the given field, then L is an algebra over K. Here, the dimension $[L : K]$ is usually called the degree of L over K.

(b) Let G be a given group written in multiplicative notation. Take a vector space A over the given field K whose dimension is equal to the cardinal number $(G : 1)$ of elements in G. Then the set J of indices i for a basis $\{\eta_i\}$ of A can be chosen as the set G itself. Define the multiplication of the basis elements by the formulas

$$\eta_g \eta_h = \eta_{gh} \qquad (g, h \in G) .$$

These are formulas of the form (8); $c_{g,h,k} = \delta_{gh,k} = 0$ for $gh \neq k$ and $= 1$ for $gh = k$, $(g, h, k \in G)$. Then, the η_g form a group under multiplication isomorphic to the group G. Hence the associativity condition (11) holds. The (associative) algebra A is called the group algebra of G over the field K.

(c) Consider an arbitrary set S of elements and let J denote the set of ordered pairs (r, s) of elements r, s of S. Choose a vector space whose basis elements are indexed by these elements (r, s) of J and define the multiplication by

$$\eta_{r,s}\eta_{t,u} = \begin{cases} \eta_{r,u} & s = t \\ 0 & s \neq t \end{cases}$$

$(r, s, t, u \in S)$. It is seen at once that the associativity condition (11) is satisfied. The corresponding algebra A consists of all elements $\alpha = \sum a_{i,j}\eta_{i,j}$ with coefficients $a_{i,j} \in K$ such that, for each α, only a finite number of $a_{i,j}$ are different from 0.

In particular, if S is a finite set, say, $S = \{1, 2, \ldots, n\}$, then the element α is called the matrix (a_{ij}) and A is the algebra of all matrices of degree n over K. For an infinite set S, we get the algebra A of all matrices which have only a finite set of coefficients different from 0 (finite-type matrices).

7. An extension of § 5.

The discussion in § 5 is extended to the case that K is an arbitrary ring (instead of a field). We discuss here formal elements $\alpha = \sum a_i \eta_i$ of the form (7) where i ranges over a set of indices, the η_i are symbols, and only a finite number of the elements a_i of K are different from 0 for each α. Two such α are to be considered as equal, if they have the same "coordinates" a_i. Addition and subtraction are defined in the obvious manner, also the product $c\alpha$ for $c \in K$. We don't usually speak of the set A of these α as a vector space over K; we have here a free K-(left)-module with the basis $\{\eta_i\}$. Again, a multiplication can be defined by the formulas (9) where the c_{ijk} are elements of K subject to the old conditions. Again, if the conditions (11) hold, the multiplication is associative and we have a ring. Note that $c(\alpha\beta) = (c\alpha)\beta$ for $\alpha, \beta \in A$, $c \in K$ while $c(\alpha\beta)$ need not to be equal to $\alpha(c\beta)$ when K is not commutative.

In particular, we can form the group ring of a group G over an arbitrary ring K and the ring of matrices (say of a fixed finite degree n) with coefficients in an arbitrary ring K.

Problems to Chapter I

1. A commutator element of a ring R is an element of the form $ab - ba$ with $a, b \in R$. Show that if x and y are elements of R and

if p is a prime number, an equation holds $(x+y)^p = x^p+y^p+z+pt$, where z is the sum of commutator elements and where t is an element of R.

2. Show that the result in 1 is not correct, if p is not a prime number.

3. A Boolean ring is a ring R such that $a^2 = a$ for every $a \in R$. Deduce that $a+a = 0$ for every $a \in R$ and that R is commutative. Show that the following two conditions are necessary and sufficient in order that a commutative ring be Boolean. [In the sufficiency part (I) is only needed for $n = 4$ and (II) only for $b = a$ and $b = a^2$.]

(I) If $a^n = 0$ for some $a \in R$ and some natural integer n, then $a = 0$.

(II) $(a+b)ab = 0$ for all $a, b \in R$.

4. A non-associative algebra L is called a Lie algebra, if

$$ab = -ba, \quad a(bc) + b(ca) + c(ab) = 0$$

for all $a, b, c \in L$. Show that if A is an associative algebra and if a new product $a \times b$ of elements a, b of A is defined by setting $a \times b = ab - ba$ (where ab and ba are the given products in A) then A is a Lie algebra with respect to this new multiplication.

5. Consider the set A of all matrices of the form

$$\alpha = \begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix}$$

where a and b are complex numbers and where $\bar{a}$, $\bar{b}$ denote the conjugate complex numbers. Show that A is a skew field. Show further that A is an algebra of dimension 4 over the field of reals. A is called the algebra of quaternions.

6. Let G denote the additive group of infinite-dimensional vectors $v = (x_1, x_2, x_3, \ldots)$ with coefficients in a given field. (It does not matter whether or not the restriction is imposed that for each v only a finite number of x_i are different from 0.) Define four mappings of G into G as follows:

$$g\colon \quad (x_1, x_2, x_3, \ldots) \longrightarrow (x_1, x_3, x_5, \ldots),$$

$$h\colon \quad (x_1, x_2, x_3, \ldots) \longrightarrow (x_2, x_4, x_6, \ldots),$$

$$q\colon \quad (x_1, x_2, x_3, \ldots) \longrightarrow (x_1, 0, x_2, 0, x_3, 0, \ldots),$$

$$r\colon \quad (x_1, x_2, x_3, \ldots) \longrightarrow (0, x_1, 0, x_2, 0, x_3, \ldots).$$

Show that g, h, q, r belong to the ring E of endomorphisms of G and that the following equations hold:

$$qg = rh = I, \quad qh = rg = \square, \quad gq + hr = I .$$

7. Let G be a non-abelian group. Find two endomorphisms whose sum is not an endomorphism.

8. Let n be a natural integer. With each subset T (including the empty set $\emptyset$) of the set $\{1, 2, \ldots, n\}$, associate a basis element e(T) of an algebra A of dimension 2^n over a given field. Define the product e(S)e(T) of two such basis elements by the formula $e(S)e(T) = \delta(S, T)e(S \cup T)$ where $\delta(S, T) = \operatorname{sign} \prod_{s \in S} \prod_{t \in T} (t-s)$. (If r is a real number, we set sign $r = 0$ for $r = 0$, sign $r = 1$ for $r > 0$, and sign $r = -1$ for $r < 0$. For $S = \emptyset$ or $T = \emptyset$ the product is to be taken as 1, i.e., $\delta(S, T) = 1$.) Show that A is an associative algebra

with a unit element. (A is called a Grassmann algebra.)

9. Let V be an n-dimensional vector space over a field K. Denote a basis of V by $e(\{1\})$, ..., $e(\{n\})$ and identify these elements with the corresponding elements of the algebra A in 8. Then V becomes a subset of A and the product of two vectors is defined in A. Show first that $v^2=0$ and that $vw = -wv$ for $v, w \in V$. Then, without using determinants, prove that if $v_1, v_2, \ldots, v_n$ are n elements of V, there exists an element D of K such that $v_1 v_2 \ldots v_n = De(\{1, 2, \ldots, n\})$ and show that $D = 0$, iff $v_1, v_2, \ldots, v_n$ are linearly independent. Finally, check that D is the determinant of the n vectors.

10. Let S be a non-empty set and let F be the ring of functions defined in S with values in the field of integers (mod 3). With each $f \in F$, associate the ordered pair (A, B) of disjoint subsets A, B of S such that $f(x) \equiv 1 \pmod 3$ for $x \in A$ and $f(x) \equiv -1 \pmod 3$ for $x \in B$. Using the ring F, define a ring P whose elements are the ordered pairs (A, B) of disjoint subsets A, B of S and express sum and product of two elements of P by means of unions, intersections, and differences of sets.

11. If the vector space in § 5 is infinite dimensional, one can try to extend the algebra A introduced there by admitting elements α in (7) for which infinitely many coordinates are different from 0. However, it is necessary to consider only elements α, β for which the sums $\sum_{i,j} a_i b_j c_{ijk}$ contain only a finite number of terms different from 0. Discuss the following three cases from this point of view:

(a) The set A of all formal Laurent series

$$\alpha = \sum_{n=-\infty}^{\infty} a_n \eta^n ,$$

with coefficients a_n in a given field K such that, for each α, only a finite number of a_n with $n < 1$ are different from 0. The multiplication of the basis elements η^n, $(n = 0, \pm 1, \pm 2, \ldots)$, is defined by $\eta^m \eta^n = \eta^{m+n}$. Show that A is a field. How does A compare with the group algebra of the infinite cyclic group?

(b) The set of all formal series of the form

$$\alpha = \sum_{n=1}^{\infty} a_n \xi^{r_n} ,$$

with coefficients a_n in a given field K such that $\{r_n\}$ is a sequence of positive real numbers, not necessarily the same for different α, with $\lim_{n \to \infty} r_n = \infty$. Again, $\xi^r \xi^s$ is to be taken as ξ^{r+s}.

(c) The set of all row-finite matrices, that is, matrices with an infinite set S of indices (§ 6, (c)) such that only a finite number of coefficients $\neq 0$ appear in each row.

12. The ring $\mathbb{Z}$ of integers can be constructed as the ring of endomorphisms of an infinite cyclic group Z. Give a somewhat similar construction which leads at once to the field $\mathbb{Q}$ of rational numbers.

Hint: Consider the set T of all homomorphisms of subgroups $\neq (0)$ of Z into Z. For each $\theta \in T$, show first that there exists a unique maximal extension $[\theta] \in T$. Let $\mathbb{Q}$ be the set of all maximal elements of T and define a suitable addition and multiplication in $\mathbb{Q}$; the rational number a/b is to correspond to the mapping $x \to ax/b$ of a suitable subgroup of Z.

13. Let R be a Boolean ring as defined in 3. Show that R is isomorphic with a subring of a Boolean ring of subsets of a given set S, § 4.

Hints: Let S denote the set of all maximal families $P = \{x_\alpha\}$ of elements x_α of R such that every finite number of elements of P has a product $\neq 0$ in R. Use Zorn's lemma to show that every $x \neq 0$ in R appears in some such P. Let $< x >$ denote the subset of S consisting of all P with $x \in P$ and study the mapping $x \rightarrow < x >$.

14. Using the ring of endomorphisms of a suitable group, show that if R is a ring with unit element, there exist elements ξ with the following properties: (I) ξ is an element of a ring S which contains R as a subring and has the same unit element. (II) $a\xi = \xi a$ for all $a \in R$. (III) If $c_0 + c_1\xi + \ldots + c_n\xi^n = 0$ with $c_i \in R$, then all c_i are 0.

15. Let p be a prime number. The rational numbers of the form a/p^n with integral a and $n = 0, 1, 2, \ldots$, form a group A under addition which contains the additive group $\mathbb{Z}^+$ of integers as a subgroup. Take $G = A/\mathbb{Z}^+$ and show that the ring E of endomorphisms of G is isomorphic with the ring of p-adic integers.

Hints: Construct a subgroup H_n of order p^n for $n = 0, 1, 2, \ldots$, and show that this yields all subgroups $H \neq G$ of G. If $\theta \in E$ is not $\square$, set $|\theta| = 1/p^n$, if θ has the kernel H_n, and set $|\square| = 0$. Show that this defines a nonarchimidean valuation on E: $|\theta_1\theta_2| = |\theta_1|\,|\theta_2|$ and $|\theta_1 + \theta_2| = \mathrm{Max}\,(|\theta_1|, |\theta_2|)$ for $\theta_1, \theta_2 \in E$. Identify the ring $\mathbb{Z}$ of integers with a suitable subring of E and show that for every $\theta \in E$ and $n = 0, 1, 2, \ldots$, there exists an $a_n \in \mathbb{Z}$, such that $|\theta - a_n| \leqq 1/p^n$. Show that the sequence $\{a_n\}$ defines a p-adic integer η and study the mapping $\theta \rightarrow \eta$.

Chapter II

PROPERTIES OF RINGS. REPRESENTATIONS.

Some of the elementary theorems on groups have analogues in the theory of rings. In particular, we examine the homomorphisms of rings.

1. Additive subgroups.

Let R be a ring. Then R is, in particular, an abelian group under addition. We shall use the notation R^+ for this group, if we wish to emphasize that the set R is to be looked upon as a group and not as a ring. If R is an algebra over a field K, we always consider R^+ as an operator group with K as domain of operators. With this understanding, everything we do applies to algebras. The case of algebras will be discussed in detail in a later chapter.

By an additive subgroup A of R, we simply mean a subgroup of R^+. Thus, A is to be a non-vacuous subset of R which is closed under subtraction and hence under addition.

If A is an additive subgroup of R, two elements λ and μ of R are congruent (mod A), $\lambda \equiv \mu \pmod{A}$, if $\lambda - \mu \in A$. The set of elements μ of R congruent to a fixed λ is the residue class of λ which will be denoted by $\lfloor \lambda \rfloor$ or by $\lfloor \lambda \rfloor_A$. The addition of residue classes is given by

$$(1) \qquad \lfloor \lambda \rfloor + \lfloor \lambda' \rfloor = \lfloor \lambda + \lambda' \rfloor ,$$

for $\lambda, \lambda' \in R$. All this is a special case of group theoretical considerations.

If $\{A_j\}$ is a family of additive subgroups of R with j ranging over a set J of indices, the sum $S = \sum_j A_j$ is defined in group theory as the set of all elements σ which can be written in the form

$$(2) \qquad \sigma = \sum_j \alpha_j ,$$

where $\alpha_j \in A_j$ for each $j \in J$ and where all but a finite number of α_j vanish. Clearly, S is the smallest additive subgroup of R which contains all A_j . If for each $\sigma \in S$, the representation (2) of the element σ is unique, the sum $\sum_j A_j$ is said to be direct and we write $S = \bullet\!\sum_j A_j$. We also may write $+$ signs with a dot on top to indicate that a sum is direct.

It is clear that the addition of additive subgroups is associative and commutative.

We now define the product $A_1 A_2 \ldots A_n$ of a finite number of additive subgroups. This will be the smallest additive subgroup which contains all products

$$\alpha_1 \alpha_2 \cdots \alpha_n$$

with $\alpha_j \in A_j$. Stated explicitly, $A_1 A_2 \ldots A_n$ consists of all elements which can be written as finite sums

$$\sum_i \alpha_1^{(i)} \alpha_2^{(i)} \cdots \alpha_n^{(i)},$$

with $\alpha_j^{(i)} \in A_j$. It is clear that the multiplication of additive subgroups is associative so that no parentheses are needed in products. Of course, A^n will denote the product of n equal factors A. The two distributive laws

$$(A_1 + A_2)A_3 = A_1A_3 + A_2A_3; \quad A_3(A_1 + A_2) = A_3A_1 + A_3A_2$$

are verified easily.

If ρ is a fixed element of R and if A is an additive subgroup, then ρA is the additive subgroup consisting of all elements $\rho\alpha$ with $\alpha \in A$. The definition of $A\rho$ is analogous.

2. Subrings.

DEFINITION 1. A subring S of a ring R is a subset which itself forms a ring, if the same addition and multiplication as in R are used.

Thus, a non-empty subset S of R is a subring, if S is closed under subtraction and multiplication. In other words, S must be an additive subgroup of R and $S^2 \subseteq S$.

3. Ideals. Residue class rings.

DEFINITION 2. An ideal H of a ring R is an additive subgroup of R which satisfies the conditions

$$(3) \qquad RH \subseteq H, \quad HR \subseteq H.$$

Since H is here an additive subgroup, the quotient group R^+/H is defined. The conditions (3) guarantee that we can define a multiplication of residue classes (mod H) in a natural manner such that we have a ring R/H. In analogy to (1), we wish to have

$$(4) \qquad \lfloor \lambda \rfloor \cdot \lfloor \lambda' \rfloor = \lfloor \lambda\lambda' \rfloor ,$$

for $\lambda, \lambda' \in R$. We have to show that the residue class on the right depends only on the residue classes $\lfloor \lambda \rfloor, \lfloor \lambda' \rfloor$ and not on the elements λ, λ' which we used as representatives. If μ is another element of $\lfloor \lambda \rfloor$ and μ' another element of $\lfloor \lambda' \rfloor$, we have $\mu = \lambda + \nu$, $\mu' = \lambda' + \nu'$ with $\nu, \nu' \in H$. Hence

$$\mu\mu' = \lambda\lambda' + \lambda\nu' + \nu(\lambda' + \nu')$$

and since $\lambda\nu' \in RH \subseteq H$, $\nu(\lambda' + \nu') \in HR \subseteq H$, we have $\mu\mu' \equiv \lambda\lambda' \pmod{H}$, that is, $\lfloor \mu\mu' \rfloor = \lfloor \lambda\lambda' \rfloor$.

Thus, the product of two residue classes is well defined. It is now easy to see that the set of all residue classes (mod H) forms a ring

R/H with the addition (1) and the multiplication (4). The residue class group R^+/H is the additive group of R/H; the associative law of multiplication and the distributive laws are immediate consequences of the corresponding laws in R. Thus, we have shown

(A) If H is an ideal of R, the residue classes (mod H) form a ring, the residue class ring R/H, if addition and multiplication of residue classes are defined by

$$\lfloor\lambda\rfloor + \lfloor\lambda'\rfloor = \lfloor\lambda+\lambda'\rfloor \ , \lfloor\lambda\rfloor\lfloor\lambda'\rfloor = \lfloor\lambda\lambda'\rfloor \quad .$$

4. Homomorphisms of rings.

DEFINITION 3. A homomorphism θ of a ring R onto a ring R_1 is a mapping θ of R onto R_1 such that

$$(5) \qquad (\alpha+\beta)\theta = \alpha\theta + \beta\theta$$

$$(6) \qquad (\alpha\beta)\theta = (\alpha\theta)(\beta\theta) \ ,$$

for all $\alpha, \beta \in R$.

If θ is a one-to-one mapping, we have an isomorphism, Chapter I, § 1.

The meaning of (5) in the definition of homorphism is that θ is a homomorphism of the group R^+ onto R_1^+. Of course, not every such homorphism of R^+ will satisfy the condition (6). If we wish to stress the distinction between a homomorphism of the group R^+ and a homomorphism of the ring R, we will refer to the former as *group-homomorphisms* or *additive homomorphisms* and to the latter as *ring homomorphisms*. The additive homomorphisms satisfy (5), while the ring homomorphisms satisfy (5) and (6).

The *kernel* N of a ring homomorphism θ is defined as the set of all elements of R which are mapped on the zero-element of R_1.

(B) If H is an ideal of the ring R, the mapping $\lambda \rightarrow \lfloor\lambda\rfloor_H$ of R onto R/H is a homomorphism π the *natural homomorphism* of R onto R/H. The kernel is H.

Proof. The fact that π is a homomorphism is expressed by the equations (1) and (4). Since the zero-element of R/H is the residue class $\lfloor 0\rfloor_H$ containing the zero element 0 of R, an element λ belongs to the kernel of π, iff $\lambda = 0$, that is, iff $\lambda \in H$.

We now prove

(C) *First Theorem on homomorphic rings*. Let θ be a homomorphism of a ring R onto a ring R_1. The kernel N is an ideal of R. Two elements of R have the same image in R_1, iff they are congruent mod N. The mapping θ^* of $R/N \rightarrow R_1$ defined by

$$\lfloor \lambda \rfloor \theta^* = \lambda\theta \,, \tag{7}$$

(for all λ) is an isomorphism of R/N onto R_1 and hence

$$R/N \approx R_1 \,. \tag{8}$$

Proof. Since a ring homomorphism is an additive homomorphism, the first theorem on homomorphic groups shows that N is an additive subgroup, that two elements of R have the same image in R_1 iff they are congruent mod N, and that θ^* is a well-defined additive isomorphism of R^{+}/N onto R_1^{+}.

If $\alpha \in N$ or $\beta \in N$, then $(\alpha\theta)(\beta\theta) = 0$ and (6) shows that $(\alpha\beta)\theta=0$, that is, that $\alpha\beta \in N$. This implies that N is an ideal of R. Finally, for $\lambda, \mu \in R$, we have

$$\lfloor \lambda\mu \rfloor \theta^* = (\lambda\mu)\theta = (\lambda\theta)(\mu\theta) = (\lfloor \lambda \rfloor \theta^*)(\lfloor \mu \rfloor \theta^*) \,,$$

and hence θ^* is a ring-isomorphism of R/N onto R_1.

The theorems (B) and (C) imply that the kernels of ring-homomorphism phisms are ideals and that every ideal appears as such a kernel. Hence we could have defined ideals as the kernels of ring-homomorphisms. This remark shows that ideals in ring theory are the analogues of normal subgroups in group theory.

The following developments are quite analogous to those in group theory.

(D) Second Theorem on homomorphic rings. Let θ be a homomorphism of a ring R onto a ring S and let N be the kernel,

1) We have a one-to-one correspondence between the set of additive subgroups $A \geqq N$ of R and the set of additive subgroups B of S such that if $A \longleftrightarrow B$, then B is the image $A\theta$ of A under θ and A is the reciprocal image $B\theta^{-1}$ of B in R,

$$A\theta = B\ , \quad A = B\theta^{-1}\ . \tag{9}$$

2) The additive subgroup $A \geqq N$ of R is a subring of R, iff B is a subring of S.

3) The additive subgroup $A \geqq N$ of R is an ideal of R, iff B is an ideal of S and in this case, A/N and B are ring isomorphic; moreover,

$$R/A \approx S/B\ . \tag{10}$$

Proof. The statement 1) is an immediate consequence of the "Second Theorem on homomorphic groups," since the ring homomorphism θ is an additive homomorphism. Since it is clear that A is closed under multiplication in (9), iff B is, we have the statement 2). Similarly, we obtain the first part of 3). If B is an ideal of S, consider the product θ_o of θ with the natural homomorphism π of S onto S/B. Then θ_o maps

$$\alpha \rightarrow \alpha\theta_0 = \lfloor \alpha\theta \rfloor_B$$

for $\alpha \in R$. Of course, θ_o is a homomorphism of R onto S/B . The element $\alpha \in R$ belongs to the kernel N_o of θ_o, iff $\lfloor \alpha\theta \rfloor_B = \lfloor 0 \rfloor_B$, that is, iff $\alpha\theta \in B$. This is so, iff $\alpha \in B\theta^{-1} = A$. Hence $N_o = A$. Applying (C), (8), to R and θ_o, we obtain (10).

There is no difficulty in giving analogues of the " Third Theorem on homomorphic groups, " the theorem of Jordan H"older-Schreier, etc., but we don't have to go into this. The proofs are quite analogous. As a matter of fact, one may consider the group case and the ring case as special cases of the same more general theorems.

5. Representation of rings.

The aim of representation theory is to study arbitrary rings by means of rings of endomorphisms of abelian groups. In the following section, the basic definitions are given.

DEFINITION 4. A representation $\mathcal{W}$ of a ring R is a homomorphism of R into the ring of endomorphisms of an abelian group.

Let V be the abelian group. As before, we use additive notation in V . With every $\alpha \in R$, there is to be associated an endomorphism $\mathcal{W}(\alpha)$ of V . The following equations will hold:

$$(11) \qquad (v_1+v_2)\mathscr{W}(\alpha) = v_1\mathscr{W}(\alpha) + v_2\mathscr{W}(\alpha) ,$$

$$(12) \qquad v\mathscr{W}(\alpha+\beta) = v\mathscr{W}(\alpha) + v\mathscr{W}(\beta) ,$$

$$(13) \qquad v\mathscr{W}(\alpha\beta) = (v\mathscr{W}(\alpha))\mathscr{W}(\beta) ,$$

for all $v, v_1, v_2 \in V$ and all $\alpha.\ \beta \in R$. Here, (11) expresses the fact that the mapping $\mathscr{W}(\alpha)\colon\ v \rightarrow v\mathscr{W}(\alpha)$ is an endomorphism of V; (12) states that $\mathscr{W}(\alpha+\beta) = \mathscr{W}(\alpha) + \mathscr{W}(\beta)$, and (13) that $\mathscr{W}(\alpha\beta) = \mathscr{W}(\alpha)\mathscr{W}(\beta)$, that is, that $\mathscr{W}$ is a ring homomorphism.

In working with a fixed representation $\mathscr{W}$, we often agree to write $v\alpha$ for $v\mathscr{W}(\alpha)$. Then V becomes what we call an R-right module as defined in

DEFINITION 5. Let R be a ring. An R-*right module* V is an (additive) abelian group V such that a product $v\alpha \in V$ is defined for all $v \in V$ and all $\alpha \in R$ for which the relations hold:

$$(\text{I}) \qquad (v_1 + v_2)\alpha = v_1\alpha + v_2\alpha ,$$

$$(\text{II}) \qquad v(\alpha+\beta) = v\alpha + v\beta ,$$

$$(\text{III}) \qquad v(\alpha\beta) = (v\alpha)\beta ,$$

for all $v, v_1, v_2 \in V$ and all $\alpha, \beta \in R$.

Thus, every representation $\mathscr{W}$ of R leads to a R-right module V

which we call the representation module of $\mathcal{H}$.. At certain occasions, it will be convenient to express by our notation whether we look upon the set V as an abelian group or as a R-right module. If we wish to stress that we take the latter point of view, we shall use the notation $V^{\cdot}$ instead of V. In dealing with R-right modules, it is to be remembered throughout that they are abelian groups with R as set of operators which satisfy the additional conditions (II) and (III). The general results on operator groups apply. These will be used freely without reference; they can be found in the appendix.

Let us start now from an arbitrary R-right module $V^{\cdot}$. For fixed $\alpha \in R$, the multiplication of an element $v \in V^{\cdot}$ with α defines a mapping $v \rightarrow v\alpha$ of $V^{\cdot}$ into $V^{\cdot}$. If we call this mapping $\mathcal{H}(\alpha)$,

$$v\mathcal{H}(\alpha) = v\alpha \quad , \tag{14}$$

it follows from (I), (II), (III) that (11), (12), (13) hold. Thus, $\mathcal{H}$ is a representation of R by endomorphisms of V considered as an abelian group. We call $\mathcal{H}$ the representation in $V^{\cdot}$.

It is now clear that the study of the representations of R is equivalent with that of the R-right modules.

If V is an abelian group, we can always turn it into an R-right module by defining $v\alpha = 0$ for all $v \in V$ and $\alpha \in R$.

The corresponding representation $\mathcal{W}$ is called a zero-representation; we have $\mathcal{W}(\alpha) = \square$ for all $\alpha \in R$.

If $V^{\cdot}$ is an R-right module and α an element of R , then $V^{\cdot}\alpha$ will denote the set of all $v\alpha$ with $v \in V^{\cdot}$. Similarly, if v is an element of $V^{\cdot}$, we denote by vR the set of all $v\rho$ with $\rho \in R$.

6. Equivalent representations. Subrepresentations and quotient representations.

As already remarked, the basic concepts of group theory apply to modules, if these are considered as R-groups. We discuss this briefly and give the terminology used for representations.

Two representations $\mathcal{W}$ and $\mathcal{M}$ of a ring R are said to be similar or equivalent , if their representation modules $V^{\cdot}$ and $W^{\cdot}$ are operator isomorphic; we write $\mathcal{W} \sim \mathcal{M}$ in this case. If a fixed operator isomorphism of $V^{\cdot}$ onto $W^{\cdot}$ is chosen and the same symbol is used for an element of $V^{\cdot}$ and its image in $W^{\cdot}$, both mappings are described by the same relations $v \rightarrow v\alpha$. This will explain why similar representations are considered as "not essentially different".

Let $\mathcal{W}$ be a representation with the representation module $V^{\cdot}$. A submodule $V^{\cdot}_0$ of $V^{\cdot}$ is of course an R-subgroup of $V^{\cdot}$. The representation $\mathcal{W}_0$ in the module $V^{\cdot}_0$ is called a subrepresentation of $\mathcal{W}$. For $\alpha \in R$, the mapping $\mathcal{W}_0(\alpha)$ is simply the restriction of $\mathcal{W}(\alpha)$ to $V^{\cdot}_0$.

We can also form the quotient $V_1^{\cdot} = V^{\cdot}/V_0^{\cdot}$. This is an R-group whose elements are the residue classes $\lfloor v \rfloor$ of elements v of $V^{\cdot}$ mod $V_0^{\cdot}$. We recall that the product $\lfloor v \rfloor \alpha$ with an operator $\alpha \in R$ is defined by $\lfloor v \rfloor \alpha = \lfloor v\alpha \rfloor$. It is checked at once that for $V_1^{\cdot}$ the conditions (II) and (III) of Definition 4 are valid and hence that $V_1^{\cdot}$ is a module, the quotient module. The representation $\mathcal{W}_1$ in $V_1^{\cdot}$ is called the quotient representation. The following simple proposition is used frequently.

(E) If $\mathcal{W}_1$ is the quotient representation in $V^{\cdot}/V_0^{\cdot}$, then $\mathcal{W}_1(\alpha) = \square$ for a given $\alpha \in R$, iff $V^{\cdot}\alpha \subseteq V_0^{\cdot}$.

Indeed, $\mathcal{W}_1(\alpha)$ maps $\lfloor v \rfloor \rightarrow \lfloor v \rfloor \alpha = \lfloor v\alpha \rfloor$. Hence $\mathcal{W}_1(\alpha) = \square$, iff $\lfloor v\alpha \rfloor$ is the zero element $\lfloor 0 \rfloor$ of $V^{\cdot}/V_0^{\cdot}$ for all $v \in V^{\cdot}$, that is, iff $v\alpha \in V_0^{\cdot}$ for all v.

7. Left modules and skew representations.

Looking at Definition 4, we will find it natural to define an R-left module ${}^{\cdot}W$ as an additive abelian group such that the product αw of an element α of the ring R and the element w of ${}^{\cdot}W$ is defined as an element of ${}^{\cdot}W$ and that the equations hold:

(I*) $\qquad \alpha(w_1 + w_2) = \alpha w_1 + \alpha w_2$

(II*) $\qquad (\alpha + \beta)w = \alpha w + \beta w$

(III*) $\qquad (\alpha\beta)w = \alpha(\beta w)$, for all $w, w_1, w_2 \in W$ and $\alpha, \beta \in R$.

Let ${}^{\cdot}W$ be an R-left module. For $\alpha \in R$, let $\mathfrak{M}(\alpha)$ be the mapping of ${}^{\cdot}W$ defined by $w \rightarrow \alpha w$, the left multiplication with α,

$$w \longrightarrow w\mathfrak{M}(\alpha) = \alpha w .$$

Condition (I*) states that $\mathfrak{M}(\alpha)$ is an endomorphism of W, that is, of the set ${}^{\cdot}W$ considered only as an additive group, not as an operator group. It follows from (II*) that

$$\mathfrak{M}(\alpha+\beta) = \mathfrak{M}(\alpha) + \mathfrak{M}(\beta) .$$

In working with (III*) we find the situation different from that in right modules. We have here

$$w\mathfrak{M}(\alpha\beta) = (\alpha\beta)w = \alpha(\beta w) = \alpha(w\mathfrak{M}(\beta)) = (w\mathfrak{M}(\beta))\mathfrak{M}(\alpha) = w\mathfrak{M}(\beta)\mathfrak{M}(\alpha) .$$

Since this holds for all w, we have

$$\mathfrak{M}(\alpha\beta) = \mathfrak{M}(\beta)\mathfrak{M}(\alpha) .$$

This leads to the following definitions:

DEFINITION 6. An anti-homomorphism θ of a ring R onto a ring R_1 is a mapping of R onto R_1 such that

$$(\alpha+\beta)\,\theta = \alpha\,\theta + \beta\,\theta , \qquad (\alpha\beta)\,\theta = (\beta\theta)\cdot(\alpha\theta) ,$$

for all $\alpha, \beta \in R$. If θ is one-to one, it is an anti-isomorphism, and if such anti-isomorphisms exist, the rings R and R_1 are said to be anti-isomorphic or reciprocal. A skew representation $\mathscr{H}$ of a ring R is an anti-homomorphism of R into the ring of endomorphisms of an abelian group W.

We may now say that the mapping $\alpha \rightarrow \mathscr{H}(\alpha)$ above is a skew representation $\mathscr{H}$ of R. Conversely, if we start from a skew representation $\mathscr{H}$ of R by endomorphisms $\mathscr{H}(\alpha)$ of an abelian group W and if we write αw for $w\mathscr{H}(\alpha)$, we turn W into a left module $'W$, the representation module of the skew representation $\mathscr{H}$.

For every ring R, there exist reciprocal rings R'. Let $'$ denote an arbitrary fixed element and consider the set of all ordered pairs $< \alpha, ' >$ of elements $\alpha \in R$ and the element $'$. For simplicity, we write α' for $< \alpha, ' >$. Define an addition and a multiplication in R' by setting

$$\alpha' + \beta' = (\alpha+\beta)'; \quad \alpha'\beta' = (\beta\alpha)'$$

for all $\alpha, \beta \in R$. Obviously, R' then is a ring and the mapping $\alpha \rightarrow \alpha'$ is an anti-isomorphism of R onto R'.

Clearly, any two reciprocal rings R' and R_1' of R are isomorphic. The reciprocal ring of R' is isomorphic to R.

Essentially, the skew representations $\mathscr{H}$ of R are the representations of R'. More precisely, if $\mathscr{H}$ is a skew representation of R, set

$$\mathcal{F}(\alpha') = \mathcal{H}(\alpha) ,$$

for $\alpha' \in R'$, i.e., for $\alpha \in R$. Then $\mathcal{F}$ is a representation of R' and all representations of R' are obtained in this form. This remark shows that it will suffice to center our attention on right modules and ordinary representations.

Remarks: 1) One may wonder why "right" and "left" should play a different role. The reason is that in writing $\theta\eta$ for the result of performing θ first and then η, we made a distinction between the left and right factor. If we had used $\theta \circ \eta = \eta\theta$ to define the product in the ring of endomorphisms, that is, if we had taken the reciprocal ring as a ring of endomorphisms, it would be the left modules which belong to representations while the right modules would belong to skew-representations.

2) If $V^{\cdot}$ is an R-right module, we cannot simply change it into an R-left module by defining αv to be $v\alpha$. Of course, for commutative rings R, this will work.

8. The regular representations.

The ring R itself may be considered as an R-right module V, if the sum v_1+v_2 of two elements $v_1, v_2 \in V = R$ is the ordinary sum in R and the product $v\alpha$ of $v \in V = R$ with $\alpha \in R$ is the ordinary product in R. If we wish to emphasize that we look upon the set R as a module in this sense, we shall use the notation $R^{\cdot}$ for this module. Similarly, the notation ${}^{\cdot}R$ will be used for R considered as an R-left module.

Of course, the right module $R^{\cdot}$ defines a representation $\mathcal{R}$ of R, called the *regular representation* of R. Similarly, the left module ${}^{\cdot}R$ defines a skew representation $\mathcal{L}$, the *regular skew representation*. Thus, for a variable $\xi \in R$ and $\alpha \in R$,

$$\mathcal{R}(\alpha): \quad \xi \longrightarrow \xi\mathcal{R}(\alpha) = \xi\alpha$$

$$\mathcal{L}(\alpha): \quad \xi \longrightarrow \xi\mathcal{L}(\alpha) = \alpha\xi .$$

In other words, $\mathcal{R}(\alpha)$ stands for "right multiplication with α" and $\mathcal{L}(\alpha)$, for "left multiplication with α".

The submodules of $R^{\cdot}$ are what we call right ideals of R and the submodules of ${}^{\cdot}R$ are the left ideals.

DEFINITION 7. A *right ideal* (abbreviated r-ideal) A of R is an additive subgroup A of R such that $AR \subseteq A$. A *left ideal* (ℓ-ideal) A of R is an additive subgroup of R such that $RA \subseteq A$.

If A is both r-ideal and ℓ-ideal of R, then it is an ideal (Definition 2).

It may be noted that, in the second theorem on homomorphic rings, further statements referring to r-ideals and ℓ-ideals can be added.

9. Imbedding of rings in rings with unit element.

(F) If R is a given ring, there exists a ring $R^{\#}$ with a unit element 1 such that R is an ideal of $R^{\#}$ and that every element σ of $R^{\#}$ has a unique representation

$$\sigma = \rho + n\,1 , \tag{15}$$

with $\rho \in R$ and n a rational integer.

First proof. Let $R^{\#}$ be the set of all ordered pairs $<\rho, n>$, $\rho \in R$, n an element of rhe ring $\mathbb{Z}$ of rational integers. Define addition and multiplication in $R^{\#}$ by

$$<\rho, n> + <\rho', n'> = <\rho + \rho', n + n'> ,$$
$$<\rho, n><\rho', n'> = <\rho\rho' + n\rho' + n'\rho , nn'> .$$

One has to check that $R^{\#}$ is a ring with the unit element $1 = <0, 1>$. Since $\rho \to <\rho, 0>$ is an isomorphism of R into $R^{\#}$, we may identify $\rho \in R$ with $<\rho, 0>$ in $R^{\#}$ and then (15) holds for $\sigma = <\rho, n>$.

Second proof. Let V be the direct sum of the groups R^{+} and $\mathbb{Z}^{+}$ the additive groups of R and of the ring $\mathbb{Z}$ of integers. Thus, V consists of the ordered pairs $<\xi, n>$ with $\xi \in R$, $n \in \mathbb{Z}$. For $\rho \in R$ define

$$[illegible] = <[illegible] + n\rho, 0>$$

It is seen at once that V then becomes an R-module V^* and the corresponding representation $\mathscr{W}$ is a ring homomorphism of R into the ring E of endomorphisms of V. If 1 is the identical mapping of V, the elements $\sigma = \mathscr{W}(\rho) + n1$ with $\rho \in R$, $n \in Z$ form a subring $R^{\#}$ of E. Here, σ maps the element $< 0, 1 >$ of V on $< \rho, 0 > + < 0, n > = < \rho, n >$.

This shows that ρ and n are uniquely determined by σ. In particular, for $n = 0$, ρ is uniquely determined by $\mathscr{W}(\rho)$, that is, $\mathscr{W}$ is an isomorphism of R into $R^{\#}$. If we identify ρ with $\mathscr{W}(\rho)$, σ has the form $\rho + n1$ and ρ and n are uniquely determined. This yields (F).

The proposition (F) often permits us to work with rings which have a unit element.

The ring $R^{\#}$ is determined by R up to an isomorphism. We shall use $R^{\#}$ as standard notation for this ring.

Perhaps, it is not superfluous to remark that if R itself has a unit element e, e no longer remains the unit element in $R^{\#}$. In fact, $1 \notin R$.

We say that a representation $\mathscr{W}$ of a ring R is *faithful*, it it is an isomorphism, i.e., if $\mathscr{W}(\rho_1) = \mathscr{W}(\rho_2)$ implies $\rho_1 = \rho_2$. The second proof of (F) shows that an arbitrary ring R possesses faithful representations $\mathscr{W}$. We prove this again in a slightly different form. We show first

(G) If a ring R has a unit element, the regular representation $\mathcal{R}$ of R is faithful.

Indeed, if ρ belongs to the kernel of $\mathcal{R}$, then $\mathcal{R}(\rho) = \square$. Since $\mathcal{R}(\rho)$ maps $\xi \rightarrow \xi\rho$, we have $\xi\rho = 0$ for all $\xi \in R$. For $\xi = 1$, this yields $\rho = 0$.

We see that it suffices to assume that R has a "left" unit element (or, still more weakly, that 0 is the only right *annihilator* of R, i.e., the only element with $R\rho = (0)$).

The proposition (G) applied to $R^{\#}$ shows that the regular representation $\mathcal{R}^{\#}$ of $R^{\#}$ is faithful. This implies that its restriction to a subring R of $R^{\#}$ is a faithful representation of R. Thus

(H) Every ring R possesses faithful representations.

If R is a ring with unit element 1, an R-right module $V^{\cdot}$ is often called *unitary*, if $v1 = v$ for all $v \in V^{\cdot}$. For the representation $\mathcal{W}$ in $V^{\cdot}$, this means that $\mathcal{W}(1)$ is the identity map I of $V^{\cdot}$,

$$\mathcal{W}(1) = I. \tag{16}$$

The following proposition shows that, in dealing with representations, it is not a very serious restriction to assume (16).

(I) Let R be a ring with unit element 1. Every R-right module

$V^{\cdot}$ is a direct sum $V^{\cdot} = V_o^{\cdot} \dotplus V_1^{\cdot}$ of submodules such that $V_1^{\cdot}$ is unitary and that $v_o R = (0)$ for all $v_o \in V_o^{\cdot}$.

Proof. The set $V_o^{\cdot}$ consisting of all elements $v_o \in V^{\cdot}$ with $v_o R = (0)$ is a submodule of $V^{\cdot}$. Likewise, the set of $v_1 \in V^{\cdot}$ with $v_1 1 = v_1$ is a submodule $V_1^{\cdot}$ as is seen easily. If $v \in V_o^{\cdot} \cap V_1^{\cdot}$, then on one hand, $v 1 = 0$, and on the other, $v 1 = v$, that is , $v = 0$. $V_o^{\cdot} \cap V_1^{\cdot} = (0)$. An arbitrary element $x \in V^{\cdot}$ can be written in the form $x=(x-x1)+x1$. For any $\alpha \in R$, then $(x - x1)\alpha = x\alpha - x\alpha = 0$, and hence $x-x1 \in V_o^{\cdot}$. Since $x1 \cdot 1 = x1$, we have $x1 \in V_1^{\cdot}$. Thus, $V^{\cdot} = V_o^{\cdot} + V_1^{\cdot}$, and as $V_o^{\cdot} \cap V_1^{\cdot} = (0)$, the sum is direct.

The representation $\mathcal{W}_o$ in $V_o^{\cdot}$ is the zero-representation. Since we have a direct sum of modules, the representation $\mathcal{W}$ in $V^{\cdot}$ is completely determined by the representation $\mathcal{W}_1$ in $V_1^{\cdot}$. For the latter, we have $\mathcal{W}_1(1) = I$.

10. Irreducible representations.

DEFINITION 8. An R-right module $V^{\cdot} \neq (0)$ is simple , if it has only the trivial submodules (0) and $V^{\cdot}$. A representation $\mathcal{W}$ of R is irreducible if it is not a zero-representation and if its representation module $V^{\cdot}$ is simple.

(J) If $V^{\cdot}$ is the representation module of an irreducible representation $\mathcal{V}$ and if $v \neq 0$ is an element of $V^{\cdot}$, then $vR = V^{\cdot}$.

Proof. The elements $v_o \in V^{\cdot}$ with $v_o R = (0)$ form a submodule $V_o^{\cdot}$. Since $V^{\cdot}$ is simple, either $V_o^{\cdot} = (0)$ or $V_o^{\cdot} = V^{\cdot}$. In the latter case, we would have $V^{\cdot}\alpha = 0$ for every $\alpha \in R$ and $\mathcal{V}$ would be a zero-representation which was excluded. Hence $V_o^{\cdot} = (0)$. This means that if $v \in V^{\cdot}$ and $v \neq 0$, then $vR \neq (0)$. Since vR is a submodule of the simple module $V^{\cdot}$, we have $vR = V^{\cdot}$, q.e.d.

We shall need the following definitions:

DEFINITION 9. A right ideal M of R is maximal if $M \neq R$ and if there does not exist a right ideal M_1 with $M \subset M_1 \subset R$.

DEFINITION 10. A right ideal T of R is regular, if there exists an element $\mathcal{E} \in R$ such that $\mathcal{E}\alpha \equiv \alpha (\mathrm{mod}\ T)$ for all $\alpha \in R$

If R has a unit element 1, every r-ideal T is regular, since we can take $\mathcal{E} = 1$.

(K) If $V^{\cdot}$ is the representation module of an irreducible representation $\mathcal{V}$ and if $v \neq 0$ is an element of $V^{\cdot}$, the set M of all elements μ of R with $v\mu = 0$ is a regular maximal r-ideal M of R and $V^{\cdot} \approx R^{\cdot}/M^{\cdot}$. Conversely, if M is a regular maximal r-ideal of R, then $R^{\cdot}/M^{\cdot}$ is the representation module of an irreducible representation.

Proof. Let θ be the mapping of R defined by

$$\rho \longrightarrow v\rho$$

Clearly, this is an operator-homomorphism of R' onto $vR = V'$, cf. (J). The kernel M consists of all $\mu \in R$ with $v\mu = 0$. Then $R'/M' \approx V'$ and since V' is simple, the theorem on homomorphic groups shows that M is a maximal submodule $\subset R'$, that is, a maximal r-ideal of R. Since $v \in V' = vR$ there exists an element $\xi \in R$ with $v = v\xi$. For all $\alpha \in R$, then $v\alpha = v\xi\alpha$. Hence $v(\alpha - \xi\alpha) = 0$ which shows that $\alpha - \xi\alpha \in M$ and hence $\alpha \equiv \xi\alpha (\mathrm{mod}\ M)$ for all α. Consequently, M is regular.

Conversely, let M be a maximal right ideal of R, that is, a maximal submodule $\subset R'$. It follows from the theory of homomorphic groups that $W' = R'/M'$ is a simple module. We have to show that if M is regular, the representation $\mathfrak{M}$ in W' is not a zero-representation. Let ξ satisfy the congruence $\alpha \equiv \xi\alpha (\mathrm{mod}\ M)$ for all $\alpha \in R$. If we had $\mathfrak{M}(\alpha) = \boxed{}$ for all α, then, by (E), $R\alpha \subseteq M$ for all α. In particular, $\xi\alpha \in M$ and, since $\alpha - \xi\alpha \in M$, this would mean $\alpha \in M$ for all $\alpha \in R$. Because of $M \neq R$, this is a contradiction and (K) is proved.

The meaning of (K) is that every irreducible representation $\mathfrak{Z}$ of R is similar to a representation with space R'/M', M a regular maximal r-ideal of R.

From now on, we shall assume that R has a unit element. We have already remarked that then every r-ideal is trivially regular.

(L) If R has a unit element 1, every irreducible representation $\mathcal{W}$ represents 1 by the identity.

Indeed, if we write the representation module $V^{\cdot}$ of $\mathcal{W}$ as a direct sum $V^{\cdot} = V_0^{\cdot} \dot{+} V_1^{\cdot}$ of submodules as in (I), it follows from the simplicity of $V^{\cdot}$ that either $V^{\cdot} = V_0^{\cdot}$ or $V^{\cdot} = V_1^{\cdot}$. The former case is impossible, since $\mathcal{W}$ is not a zero-representation. Hence $V^{\cdot} = V_1^{\cdot}$ is unitary and then $\mathcal{W}(1) = \mathcal{W}_1(1) = I$.

The result is also a consequence of (J).

So far, we have not shown that R has irreducible representations. For rings without unit elements, this would not even be true (see the Problems). For rings with unit elements, it is a consequence of the proposition:

(M) Let R be a ring with unit element 1 and let T be a right ideal $T \neq R$. There exist maximal right ideals M with $T \subseteq M \subset R$.

The proof is obtained by a standard type application of Zorn's lemma. Let $\mathfrak{X}$ be the family of all right ideals X of R with $T \subseteq X \subset R$. Since $T \in \mathfrak{X}$, $\mathfrak{X}$ is not empty. Order $\mathfrak{X}$ partially by inclusion. If $\mathfrak{L}$ is a linearly ordered subfamily of $\mathfrak{X}$, the union $C = \bigcup_{X \in \mathfrak{L}} X$

of the members X of $\mathcal{L}$ is seen to be a right ideal of R. Clearly, $T \subseteq C$. However, $1 \notin C$ since otherwise 1 would belong to some $X \in \mathcal{L}$ and then $R = 1R \subseteq XR = X$ which is not true. Hence $C \in \mathfrak{X}$. This shows that the assumptions of Zorn's lemma hold for $\mathfrak{X}$, and, consequently, there exist maximal members M of $\mathfrak{X}$. This proves (M̲).

In particular, if we take $T = (0)$, we see that there exist maximal right ideals of R. Since M is automatically regular, it follows from (K̲) that R possesses irreducible representations.

(N̲) Every ring R with a unit element possesses irreducible representations.

Incidentally, if R is a ring with a unit element 1 we have $T_1R = T_1$ for every right ideal T_1 and $RT_2 = T_2$ for every left ideal T_2. Indeed, by the definition of right ideals, $T_1R \subseteq T_1$. On the other hand, $T_1 1 \subseteq T_1R$. Hence $T_1R = T_1$. The second part is proved in the same manner.

Problems to Chapter II

1. Show that if K is a ring with unit element 1 and if A is an additive K-group such that $v(\alpha+\beta) = v\alpha + v\beta$ and $v1 = v$ for all $v \in A$; $\alpha, \beta \in K$, then A must be abelian.

2. (Jacobson) Show that if a ring R has only one left unit element e, then e is a unit element.

3. Let A and B be two additive subgroups of a ring R. Let X be the set of all elements $x \in R$ such that $Ax \subseteq B$.

(a) Show that if B is an r-ideal, so is X.

(b) Show that if A is an r-ideal, then X is an ℓ-ideal.

4. Let R be a ring with a unit element. Show that if R is the sum of an r-ideal A and an additive subgroup B which consists of nilpotent elements, then $R = A$.

5. Let K be a field, x an indeterminate. The ring of residue classes of polynomials $f(x) \in K[x]$ mod $(x-1)^2$ is an algebra R of dimension 2 over K. Choose a suitable basis and give the regular representation $\mathcal{R}(\rho)$ for an arbitrary $\rho \in R$ in matrix form.

6. If R is a given ring, V an R-right module and V_1 a submodule, there does not in general exist a submodule $V_2 \neq V$ such that $V = V_1 + V_2$. Discuss this using the example in 5.

7. Let R be the group algebra of the non-commutative group G of order 6 over the field K of complex numbers, let σ be an element of order 3 of G and τ an element of order 2. Let V be a two-dimensional vector space over K with the basis e_1, e_2. Show that

there exists a unique representation $\mathcal{W}$ of R such that $\mathcal{W}(\sigma)$ maps $e_1 \rightarrow e_2$, $e_2 \rightarrow -e_1 - e_2$ and that $\mathcal{W}(\tau)$ maps $e_1 \rightarrow e_1$, $e_2 \rightarrow -e_1 - e_2$. Similarly, show that there exists a unique representation $\mathcal{H}$ of R such that $\mathcal{H}(\sigma)$ maps $e_1 \rightarrow \rho e_1$, $e_2 \rightarrow \rho^{-1} e_2$ where ρ is a primitive third root of unity and that $\mathcal{H}(\tau)$ maps $e_1 \rightarrow e_2$, $e_2 \rightarrow e_1$. Finally, show that $\mathcal{W}$ and $\mathcal{H}$ are similar.

8. Let R be a ring and let X be a regular r-ideal $\neq$ R. Show that there exist regular maximal r-ideals $M \supseteq X$ of R.

9. Let R be the Boolean ring of the subsets of a given set S. Show that a subset X of R is an ideal $\neq$ R of R, iff the complements $S - x$ of the members x of X form a filter $\mathcal{F}$ in the sense of Bourbaki, i.e., a family $\mathcal{F} \neq \emptyset$ of subsets of S such that (1) If $M \in \mathcal{F}$ and $M_1 \supseteq M$, then $M_1 \in \mathcal{F}$. (2) If $M_1, M_2 \in \mathcal{F}$, then $M_1 \cap M_2 \in \mathcal{F}$. (3) $\emptyset \notin \mathcal{F}$.

10. The center C of a ring R is the set of all elements c of R which commute with every element of R. Show that if R is simple in the sense that R and (0) are the only ideals of R, we must have one of the three cases (I) C is a field and R is an algebra over C, (II) C = (0); (III) R consists of a prime number of elements and every product of two elements vanishes.

11. Let R be the ring of all matrices with the same infinite number of rows and columns such that in each matrix only a finite number of rows and columns is different from 0 . Show that R is simple in the sense of Problem 10 and that the center C is (0).

12. (Kaplansky, see Jacobson, Abstract Algebra I, p. 55) Prove that if an element α of a ring with a unit element e has more than one right inverse, then it has infinitely many.

13. Let R be a commutative ring in which not every element is a zero divisor. (An element $x \in R$ is a zero divisor of R , if there exists a $y \neq 0$ in R such that $xy = 0$.) Using a procedure somewhat similar to that suggested in Problem 12 of Chapter I , show that there exists a commutative ring S such that (I) R is a subring; (2) S has a unit element; (3) Every element of S which is not a zero divisor has a reciprocal in S; (4) If x is an element of S there exist two elements a, b in R such that a is not a zero divisor in S and that $ax = b$. (5) If $a \in R$ is not a zero divisor in R , then it is not a zero divisor in S .

14. Let H be an ideal of R .

(a) Show that R/H has a unit element, if H is regular as an r-ideal and regular as an ℓ-ideal (i. e., there exists $e_1, e_2 \in R$ such that $e_1\alpha \equiv \alpha$, $\alpha e_2 \equiv \alpha \bmod H$ for all $\alpha \in H$). In this case, we call H a regular ideal

(b) Show that the intersection of a regular ideal and a regular r-ideal is a regular r-ideal.

(c) The intersection of two regular r-ideals is regular, if one of them is maximal.

15. Let R and $R^{\#}$ have the same significance as in § 9.

(a) Show that a right ideal A of R is regular, iff there exists an r-ideal A_1 of $R^{\#}$ such that $A_1 \cap R = A$, $R + A_1 = R^{\#}$.

(b) Without using the results of Chapter III, show that the intersection of all maximal r-ideals of $R^{\#}$ equals the intersection of all regular maximal r-ideals of R .

16. Let R be a ring and H an ideal of R .

(a) Show that if H has a unit element, then R is the direct sum of H and another ideal.

(b) Show conversely that if a ring H has the property that every ring R containing H as an ideal is the direct sum of H and another ideal, then H has a unit element.

17. Let H be an ideal of the ring R . Consider H as a ring.

(a) Show that an r-ideal A of H need not be an r-ideal of R .

(b). Show that every regular (two-sided) ideal of H is an ideal of R .

(c) Show that if A is a regular maximal r-ideal of H, then there exists a unique regular maximal r-ideal M of R such that $M \cap H = A$.

18. Let R be the commutative ring discussed in Problem 11 (b) of Chapter I. Show that there do not exist maximal ideals in R. (Hints. Imbed R into a larger ring S consisting of all formal series $\alpha = \sum_{n=0}^{\infty} \alpha_n \xi^{r_n}$ with $a_n \in K$, $r_0 = 0 < r_1 < r_2 < \ldots$, $\lim_{n\to\infty} r_n = \infty$. Using coefficients 0, we may assume that the set of exponents $\{r_n\}$ in each α is closed under addition. Show that α has an inverse in S, iff $a_0 \neq 0$. Now show that if an ideal M of R contains an element $\gamma = c_1\xi^{s_1} + c_2\xi^{s_2} + \ldots$ with $c_j \in K$, $c_1 \neq 0$ and $0 < s_1 < s_2 < \ldots$, $s_n \to \infty$ then M contains all ξ^m with $m > s_1$).

19. Let n be a natural integer and let $\mathcal{F}$ be the set of all finite sequences $S = \{i_1, i_2, \ldots, i_r\}$ of numbers $i_\alpha = 1, 2, \ldots, n$ the empty sequence $\emptyset = \{\ \}$ is also to be considered as an element of $\mathcal{F}$ for $r = 0$. If S and T are two elements of $\mathcal{F}$, then $S + T$ is to be the sequence obtained by taking first the elements of S and then those of T. Let K be a field and associate a basis element e(S) of a vector space R over K with each $S \in \mathcal{F}$. An associative multiplication in R can be defined by setting $e(S)e(T) = e(S+T)$ for $S, T \in \mathcal{F}$, see Chapter I, § 5. This R is the tensor algebra belonging to an n-dimensional vector space over K.

Let $c_1, \ldots, c_n$ be a system of n elements of K and let H be the ideal of R generated by all the elements $e(ij) + e(ji)$ with $i \neq j$ and all the elements $e(ii) - c_i e(\emptyset)$ (i.e., H is the smallest ideal containing these elements.) The residue class algebra R/H is called a Clifford algebra A.

(a) Show that the residue classes mod H of the 2^n elements $e(i_1, i_2, \ldots, i_r)$ with $1 \leqq i_1 < i_2 < \ldots < i_r \leqq n$; $0 \leqq r \leqq n$ form a basis of A.

(b) Obtain the scalars of multiplication of A for this basis. (Suggested procedure: Assuming (a) as true, answer (b). Use your result to define an algebra A_1 of dimension 2^n and prove A_1 to be associative. Define a homomorphism of R onto A_1 with the kernel H.)

20. Let R be an algebra over a field K and let $\mathcal{V}$ be a representation of R by linear transformations of a vector space V. Let V^* be dual space of V (consisting of all linear transformations f of V into K) and let $\mathcal{V}^*(\alpha)$ denote the dual transformation of $\mathcal{V}(\alpha)$ (i.e., $\mathcal{V}^*(\alpha)$ maps $f \in V^*$ on $g \in V^*$ such that $g(v) = f(v\,\mathcal{V}(\alpha))$ for $v \in V$). Show that the $\mathcal{V}^*(\alpha)$ with $\alpha \in R$ form a skew representation $\mathcal{V}^*$ of R. Give examples to show that $\mathcal{V}$ may be irreducible and $\mathcal{V}^*$ reducible, but show that this is impossible, if V has finite dimension. What can you say about the relation between $\mathcal{V}$ and the dual $(\mathcal{V}^*)^*$ of $\mathcal{V}^*$?

Chapter III

THE RADICAL OF A RING

In a given ring R, we have a characteristic ideal N, the radical of R. The properties of the radical are studied in this chapter.

For the sake of brevity, we shall say "R-module" for "R-right module". We shall usually denote these modules by letters such as V instead of using $V^{\cdot}$.

1. Definition of the radical.

DEFINITION 1. The *radical* Rad (R) of a ring R is the subset consisting of those elements $\nu \in R$ which are represented by $\square$ in every irreducible representation of R.

If no irreducible representation of R exists, this means that Rad $(R) = R$. Then R is called a *radical ring*. If irreducible representations exist, Rad $(R) \neq R$.

Obviously, equivalent representations have the same kernel. By Chapter II, (K), every irreducible representation of R is equivalent with a representation $\mathcal{F}$ whose representation module has the form R/M where M is a regular maximal r-ideal of R. Thus, $\nu \in$ Rad (R), iff $\mathcal{F}(\nu) = \square$ for all such $\mathcal{F}$.

Incidentally, this formulation may be more comfortable to a reader who worries about getting entangled in set theoretical paradoxes. We cannot speak of the "set" of all irreducible representations of R while the representations of the type $\mathcal{F}$ certainly form a "set" and the condition $\mathcal{F}(\nu) = \square$ for all $\mathcal{F}$ defines a *subset* of R. Actually, Definition 1 is all right as it stands.

The kernel of the representation $\mathcal{F}$ with the representation module R/M consists of the elements ν such that $R\nu \subseteq M$ (Chapter II, (E)). Hence, Definition 1 can be stated as follows:

(A) An element ν of the ring R belongs to the radical Rad (R), iff $R\nu \subseteq M$ for every regular maximal r-ideal M of R.

Actually, we may drop the word "regular".

(A*) We have $\nu \in \text{Rad}(R)$, iff $R\nu \subseteq M$ for every maximal r-ideal M of R.

Indeed, for any maximal r-ideal M, the module R/M is simple and the corresponding representation is either irreducible or the zero representation. In either case, an element ν of the radical is represented by $\square$, i. e., $R\nu \subseteq M$.

Since a representation is a ring homomorphism, its kernel is an ideal. Since Rad (R) is the intersection of the kernels of the irreducible representations, we have

(B) THEOREM 1. The radical of a ring R is an ideal of R

2. Remarks about representations of a residue class ring.

Let H be an ideal of the ring R and let $R^* = R/H$ denote the residue class ring. If $\mathcal{W}^*$ is a representation of R^*, set

$$\mathcal{W}(\alpha) = \mathcal{W}^*(\lfloor \alpha \rfloor), \tag{1}$$

where $\lfloor \alpha \rfloor$ again is the residue class (mod H) of the element $\alpha \in R$. Clearly, $\mathcal{W}$ is a representation of R whose kernel includes H. Conversely, if $\mathcal{W}$ is a representation of R whose kernel includes H and if we define $\mathcal{W}^*(\lfloor \alpha \rfloor)$ by (1), then $\mathcal{W}^*$ is well defined and it is a representation of R^*. If V is the representation module of $\mathcal{W}$, we may define an R^*-module V^* consisting of the same elements as V and using the same addition by setting $v\lfloor \alpha \rfloor = v\alpha$. Then V^* is the representation module of $\mathcal{W}^*$. The elements of each submodule W of V form a submodule W^* of V^* and vice versa. In particular, V and V^* are simple at the same time. Of course $\mathcal{W}$ and $\mathcal{W}^*$ are zero-representations at the same time. Hence

(C) If H is an ideal of R, we have a one-to-one correspondence between the representations $\mathcal{W}^*$ of $R^* = R/H$ and the representations $\mathcal{W}$ of R whose kernel includes H, $\mathcal{W}(\alpha) = \mathcal{W}^*(\lfloor \alpha \rfloor)$. The representations $\mathcal{W}$ and $\mathcal{W}^*$ are irreducible at the same time.

3. Some properties of the radical.

(D) If H is an ideal of the ring R and if $N = \mathrm{Rad}\,(R)$, then

$$(H + N)/H \subseteq \mathrm{Rad}\,(R/H) \,. \tag{2}$$

Proof. Let $\lfloor \nu \rfloor$ be an element of $(H + N)/H$. Clearly, the representative ν can be chosen as an element of N. Hence $\mathfrak{W}(\nu) = \square$ for every irreducible representation $\mathfrak{W}$ of R. It follows from (C) that then $\mathfrak{W}^*(\lfloor \nu \rfloor) = \square$ for every irreducible $\mathfrak{W}^*$ of R/H and this means that $\lfloor \nu \rfloor \in \mathrm{Rad}\,(R/H)$.

(E) If H is an ideal of R and $H \subseteq N = \mathrm{Rad}\,(R)$, then

$$\mathrm{Rad}\,(R/N) = N/H \,. \tag{3}$$

Proof. If $\mathfrak{W}$ is an irreducible representation of R, its kernel includes N and hence H, on account of the assumption. Thus, $\mathfrak{W}$ is obtained from an irreducible representation $\mathfrak{W}^*$ of R/H. If $\lfloor \alpha \rfloor \in \mathrm{Rad}\,(R/H)$, then $\mathfrak{W}^*(\lfloor \alpha \rfloor) = \square$ and it follows that $\mathfrak{W}(\alpha) = \square$ for all irreducible representations $\mathfrak{W}$ of R. Hence $\alpha \in N$. This shows that $\mathrm{Rad}\,(R/H) \subseteq N/H$. The opposite inclusion is obtained from (2), since here $H + N = N$.

DEFINITION 2. A ring R is semisimple, if its radical consists only of the zero-element.

(F) THEOREM 2. If Rad (R) = N , then R/N is semisimple. If H is an ideal with R/H semisimple, then $N \subseteq H$: The radical is the smallest ideal with semisimple residue class ring.

Indeed, (E) shows for H = N that R/N is semisimple. On the other hand, if R/H is semisimple for some ideal H , then $H + N \subseteq H$ by (D), that is, $N \subseteq H$.

In general, the equality sign does not hold in (2) and, in particular, R/H need not be semisimple for $H \supset N$, see Problem 2.

(G) THEOREM 3. The radical of a ring R is the intersection of the regular maximal r-ideals of R .

Proof. Let M be a regular maximal r-ideal of R and let $\mathcal{E}$ be an element of R such that $\mathcal{E}\alpha' - \alpha \in M$ for all α . This implies that α and $\mathcal{E}\alpha$ will belong to M at the same time.

If $\nu \in$ Rad (R) , then $R\nu \subseteq M$ by (A). In particular, $\mathcal{E}\nu \in M$ and hence $\nu \in M$. Thus, Rad (R) $\subseteq M$.

On the other hand, if $\nu \notin$ Rad (R) , there exists an irreducible representation $\mathcal{W}$ of R such that $\mathcal{W}(\nu) \neq \square$. then $v\nu \neq 0$ for some v in the representation module of $\mathcal{W}$. By Chapter II (K), there exists a regular maximal r-ideal M with $\nu \notin M$.

If R has a unit element, every ideal is regular.

(G*) If R has a unit element, the radical of R is the intersection of the maximal r-ideals.

As an example, consider the ring $\mathbb{Z}$ of rational integers. If p is a prime number, then $p\mathbb{Z}$ is a maximal r-ideal. Hence if $n \in \operatorname{Rad}(\mathbb{Z})$, then n must be divisible by every prime p and this implies $n = 0$. Thus

(H) The ring $\mathbb{Z}$ of rational integers is semisimple.

4. The radical of a subring which is an ideal of R.

In general, there is not much one can say about the relationship between the radical of a subring H of R and the radical of R. The situation is different, however, if H is an ideal of R. (Of course, ideals are subrings.)

We first prove a result on representations. If $\mathcal{W}$ is a representation of R and if H is a subring of R, the restriction $\mathcal{W}_o$ of $\mathcal{W}$ to H is a representation of H. The representation module V_o of $\mathcal{W}_o$ consists of the same elements as the representation module V of $\mathcal{W}$; the operations are the same, but only operators in H are taken instead of operators in R. We show

(I) Let H be an ideal of the ring R. If $\mathcal{W}$ is an irreducible representation of R whose kernel does not include H, then the restriction $\mathcal{W}_o$ of $\mathcal{W}$ to H is an irreducible representation of H.

Every irreducible representation of H can be obtained in this manner from an irreducible representation $\mathcal{W}$ of R.

Proof. Let V be the representation module of the irreducible representation $\mathcal{W}$ of R. Let Z be the set of all $z \in V$ such that $zH = (0)$. Then Z is an additive subgroup of V. Since $RH \subseteq H$, we have $zRH \subseteq zH = (0)$ for $z \in Z$. Hence $zR \subseteq Z$, that is, Z is a submodule of V. But V is simple; we have either $Z = V$ or $Z = (0)$. In the former case, $vH = (0)$ for every $v \in V$. Then the restriction $\mathcal{W}_0$ of $\mathcal{W}$ to H is the zero representation; the kernel of $\mathcal{W}$ includes H. If this is not so, then $vH \neq (0)$ for every $v \neq 0$, $v \in V$. Since $HR \subseteq H$, the set vH is a submodule of V and as V is simple, $vH = V$ for $v \neq 0$. But this means that V remains simple, if it is considered as an H-module V_0. The restriction $\mathcal{W}_0$ of $\mathcal{W}$ to H then is irreducible, since it is not a zero-representation.

Conversely, let $\mathcal{W}_0$ be an irreducible representation of H. After replacing it by an equivalent representation, we may assume that its representation module is $V_0 = H/Z$ where Z is a regular maximal r-ideal of the ring H, cf. Chapter II, (K). Set $X = Z + ZR$. Clearly, X is an r-ideal of R. Since $Z \subset H$ and $ZR \subseteq HR \subseteq H$, we have $X \subseteq H$ and then X is also an r-ideal of H. Now, $X \supseteq Z$ and as Z was a maximal r-ideal of H, either $X = H$ or $X = Z$.

In the former case, $H = Z + ZR$ and

$$H \cdot H = ZH + ZRH \subseteq ZH + ZH \subseteq Z .$$

But then the representation $\mathcal{W}_o$ with the module H/Z would be a zero-representation (cf. Chapter II, (E)). Hence we must have $X = Z$ and Z is an r-ideal of R. The quotient H/Z of the R-modules H and Z can then be considered as an R-module V. The H-module V_o is obtained from V by taking operators only from H. Since V_o is simple, clearly V is simple. If $\mathcal{W}$ is the representation in V, then $\mathcal{W}$ is irreducible and the given representation $\mathcal{W}_o$ is the restriction of $\mathcal{W}$ to H.

As an application, we have

(J) If the subring H of R is an ideal of R, then

$$\text{Rad}\,(H) = H \cap \text{Rad}\,(R) .$$

Proof. If $\mu \in \text{Rad}\,(H)$, then $\mathcal{W}_o(\mu) = \square$ for every irreducible representation $\mathcal{W}_o$ of H and, by (I), $\mathcal{W}(\mu) = \square$ for every irreducible representation $\mathcal{W}$ of R and hence $\mu \in \text{Rad}\,(R)$. Thus, $\mu \in H \cap \text{Rad}\,(R)$. Conversely, if $\nu \in H \cap \text{Rad}\,(R)$, then $\mathcal{W}(\nu) = \square$ for every irreducible representation $\mathcal{W}$ of R. By (I), $\mathcal{W}_o(\nu) = \square$ for every irreducible representation $\mathcal{W}_o$ of H and this yields $\nu \in \text{Rad}\,(H)$.

Our result can be applied to the ring $R^{\#}$ of Chapter II, § 9 taking for H the ideal R of $R^{\#}$. This yields

$$\text{(4)} \qquad \operatorname{Rad}(R) = R \cap \operatorname{Rad}(R^{\#}) .$$

Now clearly, the residue class ring $R^{\#}/R$ is isomorphic with the ring $\mathbb{Z}$ of integers which is semisimple (cf. (H)). By (F), the ideal R of $R^{\#}$ then includes the radical of $R^{\#}$, and (4) becomes $\operatorname{Rad}(R) = \operatorname{Rad}(R^{\#})$.

(K) If R is a ring and $R^{\#}$ the corresponding extented ring with a unit element (Chapter II, § 0), then

$$\text{(5)} \qquad \operatorname{Rad}(R) = \operatorname{Rad}(R^{\#}) .$$

Because of this result, it is often enough to deal with rings with unit elements.

Remark: If H is an ideal of R, sometimes the term "the radical of H" is used for the ideal of R which corresponds to Rad (R/H) under the natural homomorphism of $R \to R/H$. Of course, this is not Rad (H).

5. The Perlis-Jacobson condition for the radical.

DEFINITION 3. An element α of a ring R is said to be quasi-right-regular (abbreviated q.r.r.), if there exists an $\alpha' \in R$ with $\alpha + \alpha\alpha' + \alpha' = 0$ and then α' is called a quasi-right-inverse (q.r.i.) of α. Similarly, α is quasi-left-regular (q.ℓ.r.), if there exists an $\alpha'' \in R$ with $\alpha + \alpha''\alpha + \alpha'' = 0$ and then α'' is a quasi-left-inverse (q.ℓ.i.) of α.

Note that if R has a unit element 1, then α has the q.r.i. α' iff $(1+\alpha)(1+\alpha') = 1$. Similarly, α'' is a q.ℓ.i. of α, iff $(1+\alpha'')(1+\alpha) = 1$.

If α' is a q.r.i. of α in R, the same is true in any ring R_1 containing R as subring. In particular, we may take R_1 as the ring $R^{\#}$ (Chapter II, § 9). Conversely, if $\alpha \in R$ has a q.r.i. $\rho + n1$ in $R^{\#}$; $\rho \in R$, $n \in \mathbb{Z}$, then $\alpha + \alpha\rho + n\alpha + \rho + n1 = 0$ which implies $n = 0$ and then ρ is a q.r.i. of α in R.

If α has both a q.r.i. α' and a q.ℓ.i. α'' in R and if we set $\beta = 1+\alpha$, $\beta' = 1+\alpha'$, $\beta'' = 1+\alpha''$ in $R^{\#}$, then $\beta\beta' = 1$, $\beta''\beta = 1$ and hence $\beta'' = \beta''(\beta\beta') = (\beta''\beta)\beta' = \beta'$. Thus, $\alpha'' = \alpha'$. In this case, we say that α is quasi-regular and that α' is a quasi-inverse of α.

(L) THEOREM 4. The radical of R consists entirely of q.r.r. elements and it includes every r-ideal of R consisting of q.r.r. elements.

Proof. Assume first that R has a unit element 1. If $\nu \in \mathrm{Rad}(R)$, form the right ideal $(1+\nu)R$. If we had $(1+\nu)R \neq R$, there would exist a maximal r-ideal M of R with $(1+\nu)R \subseteq M$ (Chapter II, (M)). Then $1+\nu \in M$, and since $\nu \in M$ by (G*), we would have $1 \in M$ and then $R = 1R \subseteq M$ which is not true. Hence $(1+\nu)R = R$. In particular $-\nu \in (1+\nu)R$ and this means that there exist elements $\nu \in R$ with $\nu' = (1+\nu)\nu'$. But then ν' is a q.r.i. of ν and ν is q.r.r. Thus, Rad (R) consists entirely of q.r.r. elements.

Suppose next that the r-ideal T of R consists of q.r.r. elements. If M is a maximal r-ideal of R and if $T \nsubseteq M$, then $M \subset M + T$. Hence the r-ideal $M + T$ must be R. It follows that there exist elements $\mu \in M$, $\tau \in T$ with $\mu - \tau = 1$. Since $\tau \in T$ is q.r.r., it has a q.r.i. τ' and then $(1+\tau)(1+\tau') = 1$. But $1 + \tau = \mu$ and $\mu(1+\tau') = 1$ implies that $1 \in M$ which again leads to $M = R$, a contradiction. Hence $T \subseteq M$ for every maximal r-ideal M of R. By (G*), $T \subseteq \mathrm{Rad}(R)$.

Hence (L) holds for rings with unit element. If R has no unit element, employ again the ring $R^{\#}$ (Chapter II, § 9). Then

(L) holds for $R^{\#}$. Since we have seen that an element α of R is q.r.r. in R, iff α is q.r.r. in $R^{\#}$, and since Rad $(R) =$ Rad $(R^{\#})$ by (K), it follows that Rad (R) consists of q.r.r. elements of R. If T is an r-ideal of R, it is an r-ideal of $R^{\#}$.. If T consists of q.r.r. elements of R, then $T \subseteq \text{Rad}\,(R^{\#}) = \text{Rad}\,(R)$. Hence (L) holds for R.

6. The radical of the reciprocal rings.

In our previous work, r-ideals were given a preferred treatment over ℓ-ideals. However, we could have worked just as well with ℓ-ideals. This fact can be expressed in the form

(M) THEOREM 5. Let $\rho \rightarrow \rho'$ be an anti-isomorphism of R onto a reciprocal ring R' (Chapter II, § 7). The radical N of R is mapped on the radical N' of R'.

Proof. If $\nu \in N$, then, by (L), ν has a q.r.i. ν_1 with $\nu + \nu\nu_1 + \nu_1 = 0$. Since $\nu\nu_1$ also belongs to the ideal N, so does $\nu_1 = -\nu - \nu\nu_1$. Hence ν_1 again has a q.r.i. ν_2. If we work again in $R^{\#}$ and set $\mu = 1 + \nu$, $\mu_1 = 1 + \nu_1$, $\mu_2 = 1 + \nu_2$, then $\mu\mu_1 = 1$, $\mu_1\mu_2 = 1$ and hence $\mu = \mu\mu_1\mu_2 = \mu_2$. Thus $\mu_1\mu = 1$ and this means that ν_1 is a q.ℓ.i. of ν. This proves that every $\nu \in N$ is q.ℓ.r.

Roughly speaking, the anti-isomorphism of R onto R' interchanges "right" and "left". Right ideals of R are mapped on left ideals of R', left ideals of R on right ideals of R'. If ρ is q.r.r. in R, then ρ' is q.ℓ.r. in R', etc. If N' is the image of the radical Rad (R) = N, then N' is an ideal of R'. Since N consists of q.ℓ.r. elements of R, every element of N' is q.r.r. in R'. Hence N' $\subseteq$ Rad (R'), by (L), applied to R'. But if we now interchange R and R' and use the inverse anti-isomorphism $\rho' \rightarrow \rho$ of R' onto R, our result shows Rad (R') then is mapped on a subset of N = Rad (R) and this means that Rad (R') $\subseteq$ N'. Hence N' = Rad (R') and this yields (M).

If we apply any of the previous results to R' and use the anti-isomorphism $\rho' \rightarrow \rho$, we obtain a result for R. For instance, Rad (R) is the intersection of the kernels of the irreducible skew representations of R. If we call an ℓ-ideal L of R "regular", if there exists an $\eta \in R$ such that $\alpha \equiv \alpha\eta$ (mod L), then an element ν belongs to Rad (R), iff $\nu R \subseteq L$ for all regular maximal ℓ-ideals L of R. Furthermore, Rad (R) is the intersection of all regular maximal ℓ-ideals of R, etc.

7. Some remarks.

We prove a few more special results which are useful.

(N) An element ν of R belongs to $N = \text{Rad}(R)$ if $\nu\rho$ is q.r.r. for all $\rho \in R$.

Proof. If $\nu\rho$ is q.r.r. for all ρ, then the r-ideal νR consists of q.r.r. elements and $\nu R \subseteq N$ by (L). The remarks at the end of § 6 shows that $\nu R \subseteq L$ for every regular maximal ℓ-ideal L of R and this implies $\nu \in N$. Conversely, if $\nu \in N$, then $\nu\rho \in N$ for every ρ and (L) shows that $\nu\rho$ is q.r.r.

It is not difficult to prove (N) without using § 6.

DEFINITION 4. An element $\eta \neq 0$ of R is an idempotent, if $\eta^2 = \eta$ and hence $\eta^n = \eta$ for every natural integer n.

(O) The radical Rad (R) does not contain an idempotent.

Proof. If $\eta \in \text{Rad}(R)$, then $-\eta \in \text{Rad}(R)$ is q.r.r. Hence there exists an η_1 such that $-\eta - \eta\eta_1 + \eta_1 = 0$. Multiply on the left with η. If $\eta^2 = \eta$, this yields $-\eta - \eta\eta_1 + \eta\eta_1 = 0$, that is, $\eta = 0$.

DEFINITION 5. An element ν of R is said to be nilpotent if $\nu^n = 0$ for some natural integer n. Similarly, an additive subgroup A of R is nilpotent, if $A^n = (0)$ for some n. Finally, A is a nilsubgroup, if A consists of nilpotent elements.

In particular, we speak of nilideals, nil-r-ideals, nil-ℓ-ideals. If A is nilpotent, it is a nilsubgroup, but the converse is not true. Indeed, $A^n = (0)$ requires that the product of any n elements of A vanishes and even if the n-th power of all elements of A vanishes, this need not be true. If ν is nilpotent, then ν is q.r.r. Indeed, if $v^n = 0$, then $\nu_1 = -\nu + \nu^2 - \nu^3 + \dots \pm \nu^{n-1}$ is a q.r.i. of ν, as shown by a simple computation. Combining this remark with (L), we have

(P) Every nil-r-ideal and nil-ℓ-ideal is included in the radical.

However, it is not true that the radical is nilpotent or even a a nilideal. A commutative ring with 0 as its only zero divisor may be its own radical, see Problem 3.

8. Rings with minimum condition.

DEFINITION 6. We say that a ring R satisfies the *minimum condition* (m-condition) for r-ideals, if every non-empty family $\mathcal{F}$ of r-ideals contains minimal members, i.e., r-ideals which do not properly include any member of $\mathcal{F}$. If the m-condition holds for r-ideals of R, we say that R is an *m-ring*.

As in all similar cases, the m-condition is equivalent with the descending chain condition: If $\{X_n\}$ is a descending chain of r-ideals $X_1 \supseteq X_2 \supseteq X_3 \supseteq \dots$, only a finite number of X_n are distinct.

We first show:

LEMMA: If $A \neq (0)$ is an additive subgroup of the radical N of an m-ring, then $A^2 \neq A$.

Proof. If $RA = (0)$, then $A^2 = (0) \neq A$. Hence we may assume that $RA \neq (0)$. Let $\mathcal{F}$ be the family of all r-ideals X of R such that $XA \neq (0)$. Since $R \in \mathcal{F}$, $\mathcal{F}$ is not empty. The m-condition implies that there exists a minimal member X_o of $\mathcal{F}$. Then if Y is an r-ideal with $Y \subset X_o$, $YA = (0)$. Let Y^* be the sum of all r-ideals $Y \subset X_o$, that is, Y^* is the r-ideal consisting of all sums $\sum y_i$ of finitely many terms y_i each of which belongs to some r-ideal $Y_i \subset X_o$. Then $y_i A = ($ and hence $Y^*A = (0)$. Since $X_o A \neq (0)$, we must have $Y^* \subset X_o$. It is now clear that Y^* is a maximal submodule of X_o. This means that X_o/Y^* is a simple module and the corresponding representation $\mathcal{X}$ is either irreducible or a zero-representation. If $\nu \in N$, we have $\mathcal{X}(\nu) = \Box$ and, by Chapter II, (E), $X_o \nu \subseteq Y^*$. Since $A \subseteq N$, it follows that $X_o A \subseteq Y^*$, and hence that $X_o A^2 \subseteq Y^*A = (0)$. But we had $X_o A \neq (0)$ and it is now clear that $A^2 \neq A$.

(Q) THEOREM 6. The radical N of an m-ring R is nilpotent.

Proof. Let $A = N^h$ be a minimal member of the family $\mathcal{F}$ consisting of all powers N^r, $r = 1, 2, \ldots$. If $N^h \neq (0)$, by the lemma, $A^2 = N^{2h} \neq A$. But since A is an ideal, $A^2 \subseteq AR \subseteq A$ and hence $N^{2h} \subset N^h$. Since N^h was minimal, this is a contradiction. Hence $N^h = (0)$, q.e.d.

(R) COROLLARY 1. In an m-ring, every nil-r-ideal T (and every nil-ℓ-ideal) is nilpotent.

Proof. By (P), $T \subseteq N$ and hence $T^h \subseteq N^h = (0)$.

(S) COROLLARY 2. In an m-ring R, an element ν belongs to the radical N, iff $\nu\rho$ is nilpotent for every $\rho \in R$.

Proof. If $\nu\rho$ is nilpotent for every $\rho \in R$, then $\nu\rho$ is q.r.r. for all ρ and (N) can be applied to show that $\nu \in N$. Conversely, if $\nu \in N$, then $\nu\rho \in N$ and hence $(\nu\rho)^h \in N^h = (0)$ for suitable h.

(T) COROLLARY 3. If S is a subring of an m-ring R, then $S \cap \mathrm{Rad}\,(R) \subseteq \mathrm{Rad}\,(S)$.

This is an immediate consequence of (S). As the examples given in the problems show, (T) does not hold for all rings.

Problems to Chapter III.

1. If R is a ring, show that $\mathrm{Rad}\,(\mathrm{Rad}\,(R)) = \mathrm{Rad}\,(R)$.

2. Let R be a commutative principal ideal domain.

   (a) What is $\mathrm{Rad}\,(R)$? When is R semisimple?

   (b) If $H = hR$ is an ideal of R $(h \in R)$, find $\mathrm{Rad}\,(R/H)$ and show that R/H need not be semisimple when R is semisimple.

3. (a) Let p be a fixed prime number and let R denote the ring of all rational numbers which can be written in the form a/b with integral a, b and $b \not\equiv 0 \pmod{p}$. Show that $\mathrm{Rad}\,(R) = pR$ and that pR is a radical ring.

   (b) The ring R in (a) is the intersection of the ring P of p-adic integers with the field $\mathbb{Q}$ of rational numbers. Show also that $\mathrm{Rad}\,(P) = pP$.

4. Let R be the ring of all n-rowed matrices M with coefficients in a given field such that each M has coefficients zero above the main diagonal. Find $N = \mathrm{Rad}\,(R)$ and determine the smallest natural integer h such that $N^h = (0)$.

5. Find the radical of a Boolean ring R . (Chapter I, Problem 3)

6. (a) Find an example of a semisimple m-ring R and an r-ideal $S \neq (0)$ such that $\mathrm{Rad}\,(S) \neq (0)$. [This shows that the relation $S \cap \mathrm{Rad}\,(R) \supseteq \mathrm{Rad}\,(S)$ does not hold in general. It also shows that there may exist nilpotent elements σ which do not lie in the radical of R . Simply take $\sigma \in \mathrm{Rad}\,(S)$, $\sigma \notin \mathrm{Rad}\,(R)$.]

(b) Find an example of a ring R and a subring S such that the relation $\mathrm{Rad}\,(S) \supseteq S \cap \mathrm{Rad}\,(R)$ is not true. (According to (T), here R cannot be an m-ring.)

(Hints: in (a), take R as a full matrix ring. In (b), take the ring in Problem 3.)

7. Let R be an algebra over a field K . Consider R just as a ring and set then $N = \mathrm{Rad}\,(R)$. Show that N is closed under multiplication with elements of K . [This implies that N is also the radical of R if considered as an algebra.]

8. Let A be an algebra with a unit element 1 over a field K . An element α of A is said to be algebraic over K , if there exists an equation $\alpha^n + c_1 \alpha^{n-1} + \dots + c_n 1 = 0$ with coefficients $c_i \in K$.

(a) Prove that if α is algebraic over K and not nilpotent, it does not lie in Rad (A) .

(*b*) Prove that if the equation above can be chosen such that $1 - c_1 + c_2 - c_3 + \ldots \neq 0$, then α has a quasi-inverse.

9. Let A be an algebra of finite dimension over a field K of characteristic γ.

(*a*) Let $\mathcal{R}$ denote the regular representation and let $\psi(\alpha)$ denote the trace of the linear transformation $\mathcal{R}(\alpha)$ for $\alpha \in A$. Show that if α is nilpotent, then $\psi(\alpha) = 0$.

(*b*) Let A be the group algebra of a group G of finite order n. Use part (*a*) to show that if $\gamma = 0$ or if γ is a prime not dividing n, then A is semisimple.

(*c*) Show that if in (*b*), γ divides n, then A is not semisimple, by showing that $\nu = \sum_{\sigma \in G} \sigma \in \text{Rad}(A)$.

10. (*a*) Let R be an m-ring. Show that if D is the intersection of an infinite number of r-ideals X_i, D is the intersection of a finite set of X_i.

(*b*) Prove that a semisimple m-ring R has a unit element.

(*Hint*: Combine part (*a*) with Problem 14 of Chapter II to show that R has a left unit element e and prove that e is a unit element.)

11. Let V be an R-module, $V \neq (0)$, and let X be an r-ideal. Show that if V contains an element v with $vX = V$, then X contains elements which are not quasi-right regular. Use this for an alternate proof of the statement that if an r-ideal X consists of quasi-right regular elements, then $X \subseteq \text{Rad}(R)$.

12. Let H be an r-ideal of a ring R. Show that if $\text{Rad}(R) = N$, $\text{Rad}(H) = T$, then T consists of the elements $x \in H$ with $xH \subseteq N$.

13. (a) Show that if a right ideal X of a ring R is not included in $\text{Rad}(R) = N$, then there exists an r-ideal Y with $Y \subset X$ and an element ρ of X with $\rho^2 \equiv \rho \not\equiv 0 \pmod{Y}$, $\rho \not\equiv 0 \pmod{N}$.

(b) Deduce that if X is an r-ideal of R with $X^h \subseteq N$ for some integer $h \geq 1$, then $X \subseteq N$.

(c) Deduce further that if X is a nilideal, then $X \subseteq N$.

(d) Show that if X and Y are two r-ideals, with $Y \subset X$, and if ρ is an element of X with $\rho^2 \equiv \rho \not\equiv 0 \pmod{Y}$, then $\rho \not\equiv 0 \pmod{N}$.

14. A representation $\mathcal{F}$ of a ring R is said to be a constituent of a representation $\mathcal{W}$, if there exist two submodules V_1 and V_2 of the representation module V of $\mathcal{W}$ such that $V_1 \supset V_2$ and that $\mathcal{F}$ is equivalent with the representation in V_1/V_2 (i.e., $\mathcal{F}$ is a quotient representation of a subrepresentation).

Let S be a subring of a ring R and assume that every irreducible representation of S is a constituent of the restriction to S of an irreducible representation of R. Show that $\text{Rad}(S) \supseteq S \cap \text{Rad}(R)$.

15. A representation $\mathcal{V}$ of a ring R is said to be completely reducible if its representation module V is a direct sum of simple modules. Assume that S is a subring of a ring R such that every irreducible representation of R has a restriction to S which is completely reducible. Show that $\mathrm{Rad}(S) \subseteq S \cap \mathrm{Rad}(R)$.

16. Let R be the group algebra of a group G over a field K of characteristic p and let S be the group algebra of a normal subgroup H of G . We may consider S as a subalgebra of R . Show that $S \cap \mathrm{Rad}(R) = \mathrm{Rad}(S)$.

17. An ideal P of a commutative ring R is said to be a prime ideal if R/P has no zero divisors except 0 . (Note that (0) may be a prime ideal.) Show that the intersection D of all prime ideals is the set of all nilpotent elements. If no prime ideals exist, then as usual in such cases, D is to be taken as R .

18. Let R be a ring and define $N_o = \mathrm{Rad}_o(R)$ as the set of all elements x of R which belong to nilpotent r-ideals.

(a) Show that N_o is an ideal of R and that $N_o \subseteq \mathrm{Rad}(R)$.

(b) If S is a subring of R , show that $S \cap \mathrm{Rad}_o(R) \subseteq \mathrm{Rad}_o(S)$.

(c) Show that if the m-condition holds for (two-sided) ideals of R , then $\mathrm{Rad}_o(R)$ is nilpotent.

19. Let R be a ring which possesses minimal r-ideals $X \supset (0)$ and let T be the sum of all these minimal r-ideals.

(a) Show that T is an ideal of R .

(b) Show that T Rad (R) = (0) and deduce that T Rad (T) = (0) , $(\text{Rad}\ (T))^2 = (0)$.

(c) Give examples to show that T need not be semisimple.

20. (Kaplansky, see Jacobson, Abstract Algebra I, p. 56.) Show that a ring R is a skew field, if every element with exactly one exception is quasi-right regular.

Chapter IV

THE STRUCTURE OF THE REGULAR REPRESENTATION

If R is a ring with unit element, the regular representation $\mathcal{R}$ of R is faithful. For this reason, $\mathcal{R}$ can be used for an investigation of R. In the present chapter, this work will be prepared by a study of the structure of $\mathcal{R}$. It will be convenient to work with the representation modules, that is here, with right ideals and quotients of right ideals. In the first three sections some useful but nearly trivial lemmas are given. From § 4 on, we consider m-rings, i. e., rings with minimum condition for r-ideals. In § 4, we assume that R has a unit element, while § 5 contains an alternate treatment which does not use this assumption.

1. Preliminaries. Schur's Lemma.

Let R be a ring and let V and W be two R-modules. We recall that an R-homomorphism θ of V into W is a mapping θ of V into W such that

$$(1) \qquad (v_1 + v_2)\theta = v_1\theta + v_2\theta; \quad (v\alpha)\theta = (v\theta)\alpha$$

for all $v, v_1, v_2 \in V$ and all $\alpha \in R$. The set of all such θ will be denoted by Hom (V, W) or $\mathrm{Hom}_R(V, W)$. If θ_1, θ_2 are two elements of Hom (V, W) , the sum $\theta_1 + \theta_2$ is defined in the usual manner by $v(\theta_1+\theta_2) = v\theta_1 + v\theta_2$ for $v \in V$ and then Hom (V, W) is an abelian group under addition. In the case $V = W$, the elements of Hom (V, W) are the R-endomorphisms of V . The ring of the R-endomorphisms of V will be denoted by $\mathcal{E}(V)$ or $\mathcal{E}_R(V)$. Thus, Hom (V, V) is the additive group $\mathcal{E}(V)^+$ of $\mathcal{E}(V)$,

$$\text{(2)} \qquad \text{Hom}\ (V,\ V) = \mathcal{E}(V)^+ .$$

If $\mathcal{V}$ and $\mathcal{W}$ are the representations in V and W , we may write Hom $(\mathcal{V}, \mathcal{W})$ for Hom (V, W) and $\mathcal{E}(\mathcal{V})$ for $\mathcal{E}(V)$. Then $v\alpha = v\,\mathcal{V}(\alpha)$, $w\alpha = w\,\mathcal{W}(\alpha)$ for $v \in V$, $w \in W$, $\alpha \in R$ and the equation (1) takes the form $(v\,\mathcal{V}(\alpha))\theta = (v\theta)\mathcal{W}(\alpha)$. Since this holds for all $v \in V$,

$$\text{(3)} \qquad \mathcal{V}(\alpha)\theta = \theta\,\mathcal{W}(\alpha) \qquad (\text{for all } \alpha \in R) ;$$

where both sides of (3) are mappings of V into W .

Thus, Hom $(\mathcal{V}, \mathcal{W})$ consists of the additive homomorphisms θ of V into W for which (3) holds. If $\mathcal{V} = \mathcal{W}$, (3) states that θ commutes with all $\mathcal{V}(\alpha)$ and for this reason, $\mathcal{E}(\mathcal{V})$ is called the commuting ring of $\mathcal{V}$.

If θ in (3) is an isomorphism of V onto W , the reciprocal mapping θ^{-1} of W onto V exists and (3) takes the form

$$(4) \qquad \theta^{-1}\mathcal{V}(\alpha)\theta = \mathcal{W}(\alpha) \qquad \text{(for all } \alpha \in R) .$$

Thus, $\mathcal{V}$ and $\mathcal{W}$ are equivalent, iff there exists an additive isomorphism θ of V onto W which satisfies (4).

(A) *LEMMA (Schur)*. If V and W are R-modules and if $\mathrm{Hom}\,(V, W) \neq (\square)$, there exists a submodule $V_o \neq V$ of V and a submodule $W_1 \neq (0)$ of W such that V/V_o and W_1 are R-isomorphic. In particular, if V and W are simple and if $\mathrm{Hom}\,(V, W) \neq (\square)$, then V and W are R-isomorphic and every $\theta \neq \square$ in $\mathrm{Hom}\,(V, W)$ is an R-isomorphism of V onto W.

This is really just the theorem on R-homomorphic groups. If V_o is the kernel of $\theta \in \mathrm{Hom}\,(V, W)$ and if $W_1 = V\theta$ is the image, then V_o is a submodule of V, W_1 is a submodule of W, and we have $V/V_o \approx W_1$. For $\theta \neq \square$, here $V_o \neq V$, $W_1 \neq (0)$. If V and W are simple, we must have $V_o = (0)$, $W_1 = W$ and θ is an R-isomorphism of V onto W.

In order to be able to state (A) conveniently in the language of representations, we say that a representation is *trivial*, if the representation module consists only of the zero element. Then (A) takes the form

(A*) If $\mathcal{V}$ and $\mathcal{W}$ are two representations of R and if $\mathrm{Hom}\,(\mathcal{V}, \mathcal{W}) \neq (\square)$, then a non-trivial quotient representation of $\mathcal{V}$ is equivalent to a subrepresentation of $\mathcal{W}$, In particular, if $\mathcal{V}$ and $\mathcal{W}$ are irreducible and $\mathrm{Hom}\,(\mathcal{V}, \mathcal{W}) \neq (\square)$, then $\mathcal{V}$ and $\mathcal{W}$ are equivalent.

If $V = W$ is simple, every $\theta \neq \square$ in $\mathrm{Hom}\,(V, V)$ has an inverse $\theta^{-1} \in \mathrm{Hom}\,(V, V)$. Thus,

(B) The commuting ring $\mathcal{C}(\mathcal{V})$ of an irreducible representation $\mathcal{V}$ is a skew field.

Actually, this is really the remark 3 in Chapter I, § 2, which states that the ring of endomorphisms of a simple Abelian operator group is a skew field.

Occasionally, a somewhat more special corollary will be useful. We say that an R-module has a greatest proper submodule V^*, if there exists a proper submodule V^* of V which includes all proper submodules of V.

(C) If the R-module V has a greatest proper submodule V^* and if W is a simple R-module, the additive groups $\mathrm{Hom}\,(V, W)$ and $\mathrm{Hom}\,(V/V^*, W)$ are isomorphic.

Indeed, if $\theta \in \mathrm{Hom}\,(V, W)$ has the kernel V_o and if $\theta \neq \square$, then $V/V_o \approx W$. As W is simple, V_o is a maximal submodule of V and hence $V_o = V^*$. If $\theta = \square$, $V_o = V$. In any case, $V_o \supseteq V^*$ and θ induces a mapping θ^* of V/V^* into W. Clearly, the correspondence $\theta \rightarrow \theta^*$ is an additive isomorphism of Hom (V, W) onto Hom $(V/V^*, W)$.

We conclude this section with another definition.

DEFINITION 1. An R-module $V \neq (0)$ is indecomposable, if it cannot be written as direct sum of two proper submodules. If V is a direct sum $V = V_1 \dot{+} V_2$ of submodules V_1 and V_2 and if $V_1 \neq (0)$, then V_1 is called a component of V. (The case $V_1 = V$ is included here.) In particular, these terms will be applied if V is an r-ideal of R.

Note that if an R-module V has a greatest proper submodule V^*, then V is indecomposable since each component $V_o \neq V$ of V is included in V^*. However, not every indecomposable module has greatest proper submodule.

In general, we use the same terminology for representations $\mathscr{W}$ as for modules V. Thus, if $V = V_1 \dot{+} V_2$ is a direct sum of submodules, the representation $\mathscr{W}$ in V is called the direct sum $\mathscr{W} = \mathscr{W}_1 \dot{+} \mathscr{W}_2$ of the subrepresentations $\mathscr{W}_1$ in V_1 and $\mathscr{W}_2$ in V_2. In this case, $\mathscr{W}$ is completely determined by $\mathscr{W}_1$ and $\mathscr{W}_2$. Moreover, $\mathscr{W}_2$ is equivalent with the quotient representation in V/V_1

(and $\mathcal{W}_1$ with that in V/V_2). If $\mathcal{W}_1$ is non-trivial, it is a component of $\mathcal{W}$.

2. Components of R.

Assume now that R is a ring with a unit element $\mathbf{1}$. This assumption will be kept to the end of § 4. Suppose that R is written as a direct sum of r-ideals

$$R = U_1 \dotplus U_2 \dotplus \dots \dotplus U_n , \tag{5}$$

where the U_i are not (0). According to Definition 1, the U_i then are components of R (really, of the R-module $R^{\cdot}$). Since $\mathbf{1} \in R$, there exist unique elements $e_1, e_2, \dots, e_n$ such that $e_i \in U_i$ and

$$\mathbf{1} = e_1 + e_2 + \dots + e_n . \tag{6}$$

We call (6) the resolution of $\mathbf{1}$ associated with the decomposition (5) of R. If $\alpha \in R$, then

$$\alpha = \mathbf{1}\alpha = e_1\alpha + e_2\alpha + \dots + e_n\alpha . \tag{7}$$

Since $e_1\alpha \in U_i$, here α is written as the sum of elements of $U_1, U_2, \dots, U_n$ and as the sum (5) is direct, this is the only way in which α can be written as such a sum.

If $\alpha \in U_j$, we obtain another such formula for α by taking the j-th term as α and all other terms as 0. This must then be the same sum as in (7) and we have

$$e_j\alpha = \alpha , \qquad e_i\alpha = 0 \qquad \text{for } \alpha \in U_j , \ i \neq j . \tag{8}$$

It follows that $U_j = e_jU_j \subseteq e_jR$ and since $e_jR \subseteq U_j$, we find

$$U_j = e_jR . \tag{9}$$

In particular, $e_j \neq 0$. Taking $\alpha = e_j \in U_j$ in (8), we obtain $e_j^2 = e_j$, $e_ie_j = 0$ for $i \neq j$. Thus, $e_1, e_2, \ldots, e_n$ are idempotents. We shall say that $e_1, e_2, \ldots, e_n$ is a system of orthogonal idempotents to indicate that $e_ie_j = 0$ for $i \neq j$.

Conversely, let (6) be any resolution of 1 into orthogonal idempotents $e_1, e_2, \ldots, e_n$. If we set $U_i = e_iR$, then U_i is an r-ideal and $e_i = e_i1 \in U_i$. The most general element u_i of U_i has the form $u_i = e_i\rho$ with $\rho \in R$ and then

$$e_iu_i = e_i^2\rho = e_i\rho = u_i; \quad e_ju_i = e_je_i\rho = 0 \quad \text{for } i \neq j .$$

In other words, e_i acts as left unit element of U_i and each e_j with $j \neq i$ is a left annihilator. Since (6) implies (7) for $\alpha \in R$, R is the sum $R = \sum_i e_iR = \sum U_i$. This sum is direct. Indeed, if

$\alpha = \sum_i u_i$ with $u_i \in U_i$, then $e_j \alpha = \sum_i e_j u_i = e_j u_j = u_j$ and u_j is uniquely determined by α. Hence (5) holds and of course (6) is the corresponding resolution of $\mathbb{1}$. This yields the result

(D) There is a one-to-one correspondence between the decompositions $R = {}^{\bullet}\sum_{i=1}^{n} U_i$ of R into direct sums of n r-ideals $U_i \neq (0)$ and the resolutions $\mathbb{1} = \sum_{i=1}^{n} e_i$ into n orthogonal idempotents e_i such that the resolution $\mathbb{1} = \sum_i e_i$ is associated with the decomposition $R = {}^{\bullet}\sum_{i=1}^{n} U_i$ with $U_i = e_i R$.

If U is a component of R and $U \neq R$, we may set $R = U_1 \dot{+} U_2$ with $U_1 = U$ and a suitable r-ideal $U_2 \neq (0)$. Hence there exists an idempotent e with $U = eR$. This is still true for $U = R$. Here $e = 1$. Conversely, let $e \neq \mathbb{1}$ be an idempotent. If we set $e_1 = e$, $e_2 = 1 - e$, we have a resolution $\mathbb{1} = e_1 + e_2$ of $\mathbb{1}$ into two orthogonal idempotents. Indeed, $e_1 e_2 = e - e^2 = 0$, $e_2 e_1 = e - e^2 = 0$, $e_2^2 = 1 - e - e + e^2 = 1 - e = e_2$. Hence eR is a component of R. This is still true for $e = 1$. Thus,

(E) Every component U of R has the form eR, where e is an idempotent. Conversely, if e is an idempotent, eR is a component of R.

We prove next

(F) LEMMA 1. Let U be a component of R and let V be an arbitrary R-module. Then $\mathrm{Hom}(U, V)$ consists exactly of the mappings $L(v)$ defined by

$$u \rightarrow vu, \tag{10}$$

where v is a fixed element of V while u ranges over all elements of U.

Proof. It is clear that $L(v) \in \mathrm{Hom}(U, V)$. Conversely, if $\theta \in \mathrm{Hom}(U, V)$ and if $U = eR$ with idempotent e, set $v = e\theta$. Then $v \in V$ and, since θ is an R-homomorphism $(eu)\theta = (e\theta)u = vu$. Now, $eu = u$ for $u \in U = eR$. Thus, $u\theta = vu$ and θ is equal to the mapping $L(v)$ in (10). This proves (F).

Since $eu = u$, it follows from (10) that $L(ve) = L(v)$. Thus, with every element ve of Ve, we have associated an element $L(ve) \in \mathrm{Hom}(U, V)$. Since $L(ve)$ maps e on $vee = ve$, ve is determined uniquely by $L(ve)$. Thus, we have a one-to-one mapping L

$$ve \rightarrow L(ve) = L(v)$$

of Ve into $\mathrm{Hom}(U, V)$. As shown by (F), L maps Ve onto $\mathrm{Hom}(U, V)$. Clearly, $L(v_1 + v_2) = L(v_1) + L(v_2)$ for v_1, v_2. Hence

L is an additive isomorphism and we have

($\underline{F_1}$) COROLLARY 1. If $U = eR$ is a component of R with idempotent e and if V is an R-module, the additive groups Ve and Hom (U, V) are isomorphic.

Consider next the case that $V = U = eR$. The elements $L(ve)$ of Hom (U, U) are the elements of the ring $\mathcal{E}(U)$ of R-endomorphisms of U, cf. (2). Each $v \in V = eR$ has the form $v = e\alpha$ with $\alpha \in R$. Thus, $\mathcal{E}(U)$ consists of the mappings $L(e\alpha e)$ with $\alpha \in R$. Here, $e\alpha e$ is an element of the set $eRe = \{e\alpha e \mid \alpha \in R\}$. Clearly, eRe is a subring of R. For $\rho, \sigma \in eRe$ and for $u \in U$, we have

$$uL(\rho)L(\sigma) = (\rho u)L(\sigma) = \sigma\rho u = uL(\sigma\rho) .$$

Hence $L(\rho)L(\sigma) = L(\sigma\rho)$ and L is an anti-isomorphism of the ring eRe onto $\mathcal{E}(U)$. This yields

($\underline{F_2}$) COROLLARY 2. If $U = eR$ is a component of R with idempotent e, the ring eRe is anti-isomorphic with $\mathcal{E}(U)$.

In particular, we may take $e = 1$, $U = R$. We use again the notation $R^{\cdot}$ for R in order to indicate that R is to be looked upon as an R-module. Here $eRe = R$ and $L(\rho)$ is the left multiplication

$\mathcal{L}(\rho)$ of the elements of R with the fixed element $\rho \in R$, cf. Chapter II, § 8 . We then have

(F_3) COROLLARY 3. If R is a ring with unit element, then $\mathfrak{L}(R^{\cdot})$ consists of the elements $\mathcal{L}(\sigma)$ of the regular skew representation $\mathcal{L}$. The rings R and $\mathfrak{L}(R^{\cdot})$ are anti-isomorphic

3. Projective modules.

Let R be a ring with unit element 1 .

$$\begin{tikzcd} & U \arrow[dl, dashed, "\varphi"'] \arrow[dr, "\psi"] & \\ V \arrow[rr, two heads, "\theta"'] & & W \end{tikzcd}$$

DEFINITION 2. An R-module U is said to be a projective module, if given any two R-modules V and W , an R-homomorphism θ of V onto W and an R-homomorphism ψ of U into W , there always exists an R-homomorphism φ of U into V such that

$$\psi = \varphi\theta . \tag{11}$$

If U , V , W are any three R-modules, if $\varphi \in \mathrm{Hom}(U, V)$ and $\theta \in \mathrm{Hom}(V, W)$, then $\varphi\theta \in \mathrm{Hom}(U, W)$. Thus $\mathrm{Hom}(U, V)\theta \subseteq \mathrm{Hom}(U, W)$. We see now that a necessary and sufficient condition for U to be projective is that, for any R-modules V and W and any R-homomorphism θ of V onto W, the equation holds

$$(11^*) \qquad \operatorname{Hom}(U, V)\theta = \operatorname{Hom}(U, W) .$$

(G̲) LEMMA 2. Every component U of a ring R with unit element is a projective module.

Proof. Let θ be an R-homomorphism of the R-module V onto the R-module W and let ψ be an R-homomorphism of U into W. According to (F̲), ψ has the form

$$\psi : u \to w_o u \qquad (\text{for all } u \in U) ,$$

where w_o is a fixed element of W. Since $V\theta = W$, there exists a $v_o \in V$ with $v_o\theta = w_o$. Again, by (F̲), the mapping φ of U given by $u \to v_o u$ belongs to $\operatorname{Hom}(U, V)$. Since θ is an R-homomorphism, $\varphi\theta$ maps

$$u \to (u\varphi)\theta = (v_o u)\theta = (v_o\theta)u = w_o u .$$

Thus, $\varphi\theta = \psi$ as required in (11).

The name "projective module" was introduced by H. Cartan-Eilenberg, Homological Algebra, Chapter I. It is quite obvious that direct sums of projective modules are projective. Since a free module is a direct sum of modules isomorphic with $R^{\cdot}$, free modules are projective. It is also easy to see that a direct summmand of a projective module is projective.

We now prove some properties of projective modules.

(H) Let U be a projective R-module , V an arbitrary R-module and V_o a submodule of V . Then

$$\text{(12)} \qquad \mathrm{Hom}\,(U,\ V)/\mathrm{Hom}\,(U,\ V_o) \approx \mathrm{Hom}\,(U,\ V/V_o)\ .$$

Proof. Let θ be the natural homomorphism of V onto V/V_o . Define a mapping Γ of Hom (U, V) into Hom $(U, V/V_o)$ by mapping $\varphi \in$ Hom (U, V) on $\varphi\theta$,

$$\Gamma\colon \varphi \to \varphi\theta\ .$$

By (11*) with $W = V/V_o$, Γ maps Hom (U, V) onto Hom $(U, V/V_o)$. Clearly, Γ is an additive homomorphism. An element φ belongs to the kernel of Γ , iff $\varphi\theta = \square$ and this will be so, iff φ maps U into the kernel V_o of θ . In that case, $\varphi \in$ Hom (U, V_o) which may be considered as a subgroup of Hom (U, V) . Now, (12) is obtained from the theorem on homomorphic groups.

(I) LEMMA 3. If U is a projective R-module and if θ is an R-homomorphism of an R-module V onto U, then V is the direct sum of the kernel V_o of θ and a submodule X of V which is R-isomorphic to U.

Proof. Take $W = U$ in Definition 2, and take ψ as the identity map of U in (11). It follows that there exists a $\varphi \in \mathrm{Hom}(U, V)$ such that

$$\begin{tikzcd}
& U \arrow[dl, "\varphi"'] \arrow[dr, "I"] & \\
V \arrow[rr, two heads, "\theta"'] & & U
\end{tikzcd}$$

$$\varphi\theta = I . \qquad (13)$$

Let X be the image of φ. Then $X\theta$ is a submodule of U and it follows from (13) that $X\theta = U$. If v is an element of V, then $v\theta \in U = X\theta$ and hence there exists an $x \in X$ with $v\theta = x\theta$. Then $v - x$ belongs to the kernel V_o of θ. This shows that $V = V_o + X$.

In order to show that this sum is direct, let $t \in V_o \cap X$. Since $t \in X = U\varphi$, there exists a $u \in U$ with $t = u\varphi$. Now (13) yields $t\theta = u\varphi\theta = u$. Since t belongs to the kernel V_o of θ, we have $u = 0$ and hence $t = u\varphi = 0$. Thus, $V_o \cap X = (0)$; the sum $V = V_o \dotplus X$ is direct. Since θ maps X onto U and since X intersects the kernel V_o of θ in (0), the restriction of θ to X is an R-isomorphism of X onto U.

(I*) COROLLARY. If V is an indecomposable module, any R-homomorphism θ of V onto a projective module $U \neq (0)$ is an isomorphism.

Indeed, V is the direct sum of the kernel V_o of θ and some module X and since $V_o \neq V$, we have $V_o = (0)$.

(J)* Let U be a projective module. Assume that U is the sum $U = B+C$ of two submodules, but that for every proper submodule B_o of B and every proper submodule C_o of C, we have $B_o + C \neq U$, $B + C_o \neq U$. Then the sum $U = B + C$ is direct.

Proof. If $D = B \cap C$, we have to show that $D = (0)$. It will be sufficient to construct a $\varphi \in \mathrm{Hom}(U, B)$ such that:

(α) $u\varphi \equiv u \pmod{C}$ for all $u \in U$; (β) $B\varphi = B$;

(γ) $c\varphi = 0$ for all $c \in C$.

Indeed, if we have such a φ and if $d \in B \cap C$, then by (β) there exists $b \in B$ with $b\varphi = d$. Since $d \in C$, then $b\varphi \equiv 0 \pmod{C}$ and, by (α), $b \equiv 0 \pmod{C}$. It now follows from (γ) that $b\varphi = 0$, that is, $d = 0$. Thus, $D = (0)$.

We now construct a φ with the required properties. If $u \in U=B+C$, we may set $u = b+c$ with $b \in B$, $c \in C$. If also $u = b_1+c_1$ with $b_1 \in B$, $c_1 \in C$, then $b - b_1 = c_1 - c$ and hence $b-b_1 \in B \cap C = D$. Thus, the residue class $\lfloor b \rfloor$ of $b \pmod{D}$ is uniquely determined by u and we can define a mapping ψ of U into B/D be setting

---

* If the alternate method of § 5 is used, this proposition is not needed.

$$(14) \qquad \psi : u \rightarrow \lfloor b \rfloor .$$

Clearly, $\psi \in \mathrm{Hom}\,(U, B/D)$. Let θ be the natural homomorphism of B onto B/D. Since U is projective, there ecists a $\varphi \in \mathrm{Hom}\,(U, B)$ with $\varphi\theta = \psi$. We claim that φ has the required properties ($\underline{\alpha}$), ($\underline{\beta}$), ($\underline{\gamma}$).

Since $\varphi\theta$ maps u on $(u\varphi)\theta = \lfloor u\varphi \rfloor$, comparison with (14) yields $\lfloor u\varphi \rfloor = \lfloor b \rfloor$, that is, $u\varphi \equiv b \pmod{D}$. Since $u = b+c \equiv b \pmod{C}$ and since $D \subseteq C$, we have $u\varphi \equiv b \equiv u \pmod{C}$. This is ($\underline{\alpha}$). In particular, if $u = b \in B$, we have $b \equiv b\varphi \pmod{C}$ and hence $B \subseteq B\varphi + C$. Since φ mapped U into B, the image $B\varphi$ of B is a submodule B_o of B and $U = B+C = B_o+C$. It now follows from the assumption of (J) that $B_o = B$, that is, $B\varphi = B$ as required by ($\underline{\beta}$). Finally, let C_o be the kernel of φ. If $c_o \in C_o$, then ($\underline{\alpha}$) for $u = c_o$ yields $c_o \equiv c_o\varphi \pmod{C}$. Since $c_o\varphi = 0$, $c_o \in C$. Hence $C_o \subseteq C$. For an arbitrary $u \in U$, we have $u\varphi \in B$ and, by ($\underline{\beta}$), there exists an element $b \in B$ with $u\varphi = b\varphi$. Then $u - b \in C_o$. Hence $U = B+C_o$. Since C_o is a submodule of C, the assumptions of ($\underline{J}$) imply that $C_o = C$.

But then $C\varphi = (0)$; $(\underline{\gamma})$ holds and the proof is complete.

4. Indecomposable components of an m-ring with unit element.

Let R be an m-ring with unit element $\mathbf{1}$ (Chapter III, § 8). For some of our results, weaker assumptions suffice, but rather than change our basic assumptions repeatedly, we prefer to indicate the modified results in "Remarks" following the theorems.

A standard argument yields

$(\underline{K}_o)$ Every r-ideal $A \neq (0)$ of an m-ring R can be written as a direct sum of a finite number of idecomposable r-ideals.

Indeed, if $(\underline{K}_o)$ is false, let α be the family of all r-ideals A of R for which $(\underline{K}_o)$ does not hold and choose A, as a minimal member of α. Then $(\underline{K}_o)$ does not hold for A and, in particular, A cannot be idecomposable. Hence there exist r-ideals B and C with $A = B \dot{+} C$, $B \subset A$, $C \subset A$. Then $B, C \notin \alpha$. But this means that B and C are direct sums of a finite number of idecomposable r-ideals and if we substitute this in $A = B \dot{+} C$, we see that A also is a direct sum of a finite number of idecomposable r-ideals, a contradiction.

Remark. The existence of a unit element is not needed for the proof of $(\underline{K}_o)$.

The proposition ($\underline{K}_o$) holds in particular for $A = R$:

($\underline{K}$) Each m-ring R is a direct sum

(15) $$R = {}^{\bullet}\sum_{i=1}^{n} U_i$$

of indecomposable components.

A decomposition (15) of R of this kind will be termed a full decomposition of R .

As shown by ($\underline{D}$) the decomposition (15) corresponds to a resolution

(16) $$1 = e_1 + e_2 + \dots + e_n$$

of of the unit element 1 of R into orthogonal idempotents.

We call an idempotent e indecomposable , if e cannot be written as a sum of two orthogonal idempotents. It is clear that e is indecomposable, iff the r-ideal eR is indecomposable.

In working with the representations of R , the irreducible representations $\mathcal{F}$ of R are of prime importance. A second important class are the indecomposable components of the regular representation $\mathcal{R}$, i.e., the representations whose representation modules are the indecomposable components J of R. We now investigate the properties of these representations and their modules.

(L) THEOREM 1. Let R be an m-ring with 1. Every indecomposable component U of R has a greatest proper submodule $W = U \cap \mathrm{Rad}(R)$.

Proof 1) If e is an idempotent in U, then $e \notin \mathrm{Rad}(R)$, (Chapter III, (0)). Hence $e \notin W$ and W is a proper submodule of U.

2) We show next that if B and C are proper submodules of U, the equation

$$U = B + C \tag{17}$$

is impossible. Since U is indecomposable, the sum here can certainly not be direct. We claim that in an equation (17) one of the modules B, C can be replaced by a proper submodule in (17). Indeed, if this could not be done, (J) would apply (as U is projective by (G)) and the sum (17) would be direct. Hence, we have an equation $U = B_1 + C_1$ where B_1 and C_1 are submodules, $B_1 \subseteq B$, $C_1 \subseteq C$ and at least one inequality holds. Apply the same argument to $U = B_1 + C_1$, etc. We find two sequences of submodules

$$B \supseteq B_1 \supseteq B_2 \supseteq \dots \; ; \; C \supseteq C_1 \supseteq C_2 \supseteq \dots ,$$

such that for each m, $U = B_m + C_m$ and either $B_m \supset B_{m+1}$ or $C_m \supset C_{m+1}$. Now submodules of $U \subseteq R$ are r-ideals. Because of the m-condition, both families $\{B_m\}$ and $\{C_m\}$ have minimal members and we obtain a contradiction. Thus, equations (17) are impossible.

3) Let B be any proper submodule of U. We have to show $B \subseteq \mathrm{Rad}\,(R)$, that is, we have to prove that, if $b \in B$, then $\mathcal{F}(b) = \Box$ for every irreducible representation $\mathcal{F}$ of R.

Suppose this was not true. If F is the representation module of $\mathcal{F}$, then $Fb \neq (0)$. Then there exist $f \in F$ with $fb \neq 0$. Since fB is a submodule of the simple module F and $fB \neq (0)$, we have $fB = F$. Set

$$C = \{\, c \mid fc = 0 ,\ c \in U \,\} .$$

Clearly, C is a submodule of U and as $b \notin C$, C is proper. For any $u \in U$, $fu \in F = fB$. This means that there exist $b_o \in B$ with $fu = fb_o$. Then $u - b_o \in C$ and hence $u \in B + C$, $U = B + C$. Since we have shown in 2) that U is not the sum of two proper submodules B and C, this is impossible.

This proves that if B is a proper submodule of U, then $B \subseteq \mathrm{Rad}\,(R)$. Hence, $B \subseteq U \cap \mathrm{Rad}\,(R) = W$ and W is the greatest proper submodule of U.

Remark . Instead of assuming the m-condition for r-ideals, the proof of (L) shows that it is sufficient to assume the m-condition for submodules of the given module U .

(M) THEOREM 2. Let R be an m-ring with 1 . Let U be an indecomposible r-ideal such that $U \not\subseteq \mathrm{Rad}(R)$. Then U is a component of R . If $R = {}^{\bullet}\sum_i U_i$ is a full decomposition of R , then U is R-isomorphic with some U_i .

Proof. Let $1 = \sum_i e_i$ be the resolution of 1 belonging to $R = {}^{\bullet}\sum U_i$; $U_i = e_i R$. Since $U = 1U = \sum_i e_i U$ and $U \not\subseteq \mathrm{Rad}(R)$, some $e_i U \not\subseteq \mathrm{Rad}(R)$. Define a mapping θ of U into U_i by letting

$$(18) \qquad \theta:\ u \longrightarrow e_i u .$$

Clearly, $\theta \in \mathrm{Hom}(U, U_i)$. The image $U\theta = e_i U$ is not included in the greatest proper submodule $U_i \cap \mathrm{Rad}(R)$ of U_i and hence $U\theta = U_i$. By (I*) θ then is an R-isomorphism; $U \approx U_i$. Moreover, there exists an $e \in U$ with $e\theta = e_i$. By (18) , $e_i e = e_i$. Then $e_i e^2 = e_i e = e_i$ and since the isomorphism θ maps both e and e^2 on e_i , $e^2 = e$. Since e cannot be 0 , e is an idempotent. Furthermore,

$$(eR)\theta = (e\theta)R = e_i R = U_i = U\theta .$$

Hence $eR = U$ and now (E) shows that U is a component of R as we had to show.

If U is an indecomposable component of R and W its greatest proper submodule, then $F = U/W$ is a simple unitary module, that is, the module of an irreducible representation $\tilde{f}$. We shall now construct a full system of non-isomorphic such modules.

(N) THEOREM 3. Let R be an m-ring with 1. Let U and U^* be two indecomposable components of R and let W and W^* be their greatest proper submodules. Then the modules U and U^* are R-isomorphic, if and only if the simple modules $F = U/W$ and $F^* = U^*/W^*$ are R-isomorphic.

Proof. If χ is an R-isomorphism of U onto U^*, then χ maps the greatest proper submodule W of U onto the greatest proper submodule W^* of U^*. This implies $U/W \approx U^*/W^*$.

Conversely, let ω be an R-isomorphism of F onto F^*. Let θ be the natural homomorphism $U \twoheadrightarrow U/W = F$ and let θ^* be the natural homomorphism $U^* \twoheadrightarrow U^*/W^* = F^*$. Then $\theta\omega \in \mathrm{Hom}\,(U, F^*)$. Since U is projective and since θ^* maps U^* onto F^*, there exists a $\varphi \in \mathrm{Hom}\,(U, U^*)$ with

$$\begin{tikzcd}
U \arrow[r, dashed, "\varphi"] \arrow[d, two heads, "\theta"'] & U^* \arrow[d, two heads, "\theta^*"] \\
F \arrow[r, two heads, "\omega"'] & F^*
\end{tikzcd}$$

$$\varphi\theta^* = \theta\omega .$$

Since $\theta\omega$ maps U onto F^*, we have $\varphi\theta^* \neq \square$. Hence φ does not map U into the kernel W^* of θ^*. Thus, the submodule $U\varphi$ of U^* is not included in the greatest proper submodule of U^* and we must have $U\varphi = U^*$. Now, (I*) shows that φ is an R-isomorphism of U onto U^*.

Remark. The proof of (N) works, when R is a ring with unit element and U and U^* are projective modules which have greatest proper submodules W and W^*.

Let $X_1, X_2, \ldots, X_k$ be a set of indecomposable components of R such that $X_i \not\cong X_j$ for $i \neq j$. If $R = {}^{\bullet}\sum_{i=1}^{n} U_i$ is a full decomposition of R, it follows from (M) that each X_j is R-isomorphic with some U_i and, of course, different X_j are R-isomorphic with different U_i. Hence $k \leqq n$.

DEFINITION 3. Let R be an m-ring with 1 and suppose that there exist k but not more than k indecomposable components $X_1, X_2, \ldots, X_k$ such that X_i and X_j are not R-isomorphic. Then k is called the height of R.

The preceding remark shows that we may assume that $X_1, X_2, \ldots, X_k$ occur as summands in a given full decomposition of R.

(O) THEOREM 4. Let R be an m-ring with 1 of height k and let $X_1, X_2, \ldots, X_k$ be a system of k indecomposable components of R such that each indecomposable component U of R is R-isomorphic to exactly one X_i. Each simple unitary module F is R-isomorphic to exactly one of the k modules $F_i = X_i/Y_i$ with $Y_i = X_i \cap \mathrm{Rad}\,(R)$.

Proof. Let $R = {}^{\bullet}\sum_i U_i$ be a full decomposition of R. If $f_o \in F$, $f_o \neq 0$, then $f_o R \neq (0)$ and hence $f_o U_j \neq (0)$ for some j. Since F is a simple module and $f_o U_j \subseteq F$, this implies $f_o U_j = F$. In other words, the mapping

$$\theta: \quad u \rightarrow f_o u$$

of U_j maps U_j onto F. Clearly, $\theta \in \mathrm{Hom}\,(U_j, F)$. If T is the kernel of θ, $U_j/T \approx F$. As F was simple, T is a maximal submodule of U_j and hence T is the greatest proper submodule $T = W_j = U_j \cap \mathrm{Rad}\,(R)$. Thus $F \approx U_j/W_j$. Now, U_j is R-isomorphic with exactly one of the modules $X_1, X_2, \ldots, X_k$. It follows from (N) that U_j/W_j and then F is R-isomorphic to exactly one of the modules $X_1/Y_1, X_2/Y_2, \ldots, X_k/Y_k$.

It is a simple matter of rephrasing to state our results in the language of representations. We shall say that representations are "distinct" in quotation marks if they are not equivalent. Then our results are summarized in the following theorem.

(P) Let R be an m-ring with 1, of height k. There exist exactly k "distinct" indecomposable components $\mathfrak{X}_1, \mathfrak{X}_2, \ldots, \mathfrak{X}_k$ of the regular representation $\mathcal{R}$ of R. Each $\mathfrak{X}_i$ possesses a unique irreducible quotient representation $\mathfrak{F}_i$. The k irreducible representations $\mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_k$ are "distinct". Each irreducible representation $\mathfrak{F}$ of R is equivalent to one of the $\mathfrak{F}_i$.

In the notation of (O), we may choose $\mathfrak{X}_i$ as the representation in X_i and $\mathfrak{F}_i$ as that in F_i.

5. Arbitrary m-rings.

If we now consider an m-ring R without assuming that R has a unit element, some modifications in the results of the preceding section become necessary. Of course, R can be imbedded in the extended ring $R^{\#}$ with unit element (Chapter II, § 9), but $R^{\#}$ is not an m-ring. Still the methods of § 4 can be adapted to this situation as is indicated in Problem 25. We prefer to use here a different approach which leads more quickly to the desired results.

If X is an r-ideal, we shall say that X is *potent*, if X is not nilpotent. In the case of an m-ring R, X is potent, iff $X \not\subseteq \mathrm{Rad}(R)$, cf. Chapter III (P), (Q). It follows from the m-condition that every potent r-ideal X includes a minimal potent r-ideal U, i.e., a potent r-ideal U of R such that every r-ideal Y of R with $Y \subset U$ is nilpotent.

($\underline{Q}$) Every minimal potent r-ideal U of an m-ring R contains idempotents e. For each such e, $U = eR$.

Proof. 1) There exist elements $u \in U$ such that $uU = U$. Indeed, if the r-ideal uU is properly included in the minimal potent r-ideal U, then $uU \subseteq \mathrm{Rad}(R)$. If this was true for all $u \in U$, we would have $U^2 \subseteq \mathrm{Rad}(R)$, and U^2 and hence U would be nilpotent. This is not true.

2) Choose then some $u \in U$ with $uU = U$. It follows that there exist $\eta \in U$ with

$$u\eta = u .$$

Hence $u\eta U = uU = U \not\subseteq \mathrm{Rad}(R)$. This implies $u \notin \mathrm{Rad}(R)$, $\eta \notin \mathrm{Rad}(R)$. In particular, $u \neq 0$, $\eta \neq 0$. Furthermore, $u\eta^2 = u\eta$,

$$u(\eta - \eta^2) = 0 . \tag{19}$$

The set Y consisting of the elements $y \in U$ with $uy = 0$ is an r-ideal $Y \subseteq U$. As $u\eta = u \neq 0$, we have $\eta \notin Y$. It follows that

$Y \subset U$ and this implies $Y \subseteq \mathrm{Rad}\,(R)$. By (19), $\eta - \eta^2 \in Y$, and we obtain

$$(20) \qquad \eta^2 \equiv \eta \not\equiv 0 \quad (\mathrm{mod}\ \mathrm{Rad}\,(R)\,)\,.$$

Moreover, since Y is nilpotent, there exist positive integers h with $Y^h = (0)$. It follows that

$$(21) \qquad (\eta - \eta^2)^h = 0\,.$$

3) If R is semisimple, (20) shows that η is an idempotent. In order to be able to deal with the general case we interrupt the proof by some auxiliary considerations. Let $\mathbb{Z}\,[t]$ denote the ring of polynomials of an indeterminate t with coefficients in the ring $\mathbb{Z}$ of rational integers. If $f \in t\,\mathbb{Z}\,[t]$, i.e., if f has the form $f = a_1 t + a_2 t^2 + \ldots + a_n t^n$ with $a_i \in \mathbb{Z}$, and if η is an element of a ring S, we set

$$f(\eta) = a_1 \eta + a_2 \eta^2 + \ldots + a_n \eta^n\,.$$

Clearly, the mapping $f \Rightarrow f(\eta)$ is a ring homomorphism of $t\,\mathbb{Z}\,[t]$ into S. This means that every integral rational relation between elements of $t\,\mathbb{Z}\,[t]$ remains correct, if t is replaced by η.

4) Determine now $f \in \mathbb{Z}[t]$ such that, in $\mathbb{Z}[t]$,

$$(22) \qquad f \equiv 0 \pmod{t^{h+1}}; \quad f \equiv 1 \pmod{(1-t)^h}.$$

In order to see that such f exist, we expand $1 = 1^{2h} = (t + (1-t))^{2h}$ by means of the binomial theorem. This gives the identity

$$1 = t^{2h} + 2ht^{2h-1}(1-t) + \ldots + (1-t)^{2h}$$

in which every term on the right is either divisible by t^{h+1} or by $(1-t)^h$. If f is the sum of the terms of the first kind, f satisfies (22).

It follows from (22) that both $f(f-1)$ and $t^{h+1}(f-1)$ are divisible by $t^{h+1}(1-t)^h = t(t-t^2)^h$. Hence, we may set

$$(23) \qquad f^2 - f = (t - t^2)^h g,$$

$$(24) \qquad t^{h+1}f - t^{h+1} = (t-t^2)^h g_1,$$

with $g, g_1 \in t\,\mathbb{Z}[t]$.

5) If η is determined as in 2) and if the polynomial f is determined as in 4), set $e = f(\eta)$. Since $\eta \in U$, it follows that $e \in U$. Moreover, replacing t by η in (23), (24) and using (21),

we find $e^2 - e = 0$ and $\eta^{h+1} e - \eta^{h+1} = 0$. The former equation shows that e is an idempotent, if $e \neq 0$. If we had $e = 0$, the latter equation would yield $\eta^{h+1} = 0$ while by (20), $\eta \equiv \eta^2 \equiv \eta^3 \equiv \ldots \equiv \eta^{h+1}$ and hence $\eta^{h+1} \not\equiv 0 \pmod{\mathrm{Rad}\,(R)}$. Thus, $e \neq 0$ and $e \in U$ is an idempotent.

6) If e is any idempotent in U, then $e = e^2$ belongs to the r-ideal $eR \subseteq U$. Since then eR cannot be nilpotent, we must have $eR = U$.

This completes the proof of (Q).

(R) If U is a minimal potent r-ideal of R and if $X \supseteq U$ is an r-ideal of $R^{\#}$, then U is a component of X (i.e., X is a direct sum of U and some other submodule).

Proof. By (Q), there exist idempotents e with $eR = U$. For $x \in X$, we have the "Peirce decomposition"

$$x = ex + (x - ex) .$$

Here, $ex = eex \in eR = U$. Further, $e(x-ex) = ex - ex = 0$. The elements $y \in X$ with $ey = 0$ form an r-ideal $Y \subseteq X$. Since $x - ex \in Y$, we have $X = U+Y$. If $y \in U \cap Y$, then y has the form $y = e\rho$ with $\rho \in R$. Since $ey = ee\rho = e\rho = y$, it follows from $ey = 0$ that $y = 0$. Thus, $U \cap Y = (0)$ and the sum $X = U \dot{+} Y$ is direct.

(S) If R is an m-ring and if $R^{\#}$ is the corresponding extended ring, there exist minimal potent r-ideals $U_1, U_2, \ldots, U_n$ of R and an r-ideal U_o of $R^{\#}$ such that

$$(25) \qquad R^{\#} = U_o \dot{+} U_1 \dot{+} \ldots \dot{+} U_n$$

and that $U_o \cap R \subseteq \mathrm{Rad}\,(R)$.

Proof. If Rad (R) = R , set $U_o = R^{\#}$. Then $U_o \cap R = R \subseteq$ Rad (R) . If $R \neq$ Rad (R), let U_1 be a minimal potent r-ideal of R . By (R), there exists an r-ideal Y_1 of $R^{\#}$ such that $R^{\#} = U_1 \dot{+} Y_1$. Suppose we have already found minimal potent r-ideals $U_1, U_2, \ldots, U_h$ of R and r-ideals $Y_1, Y_2, \ldots, Y_h$ of $R^{\#}$ such that

$$(26) \qquad R^{\#} = U_1 \dot{+} U_2 \dot{+} \ldots \dot{+} U_j \dot{+} Y_j$$

for j = 1, 2, ..., h and that

$$(27) \qquad Y_1 \cap R \supset Y_2 \cap R \supset \ldots \supset Y_h \cap R \,.$$

If the r-ideal $Y_h \cap R$ of R is potent, choose U_{h+1} as a minimal potent r-ideal with $U_{h+1} \subseteq Y_h \cap R$. By (R), there exists an r-ideal Y_{h+1} of R with $Y_h = U_{h+1} \dot{+} Y_{h+1}$. If we substitute this in (26) for j = h , we see that (26) holds for j = h+1 . Further, U_{h+1} is included in $Y_h \cap R$ but not in $Y_{h+1} \cap R$ and as $Y_h \supseteq Y_{h+1}$, we have

$$Y_h \cap R \supset Y_{h+1} \cap R ,$$

extending (27) . This process can not go on indefinitely since this would give an infinite strictly descending sequence $\{Y_m \cap R\}$ of r-ideals of R , contrary to the m-condition. It follows that, for suitable $j = n$, a formula (26) holds with $Y_n \cap R \subseteq \mathrm{Rad}(R)$. We obtain (S) by setting $U_o = Y_n$.

We supplement (S) by some remarks.

(S*) If the assumptions and the notation are as in (S), then U_o is indecomposable.

Proof. Let $\mathbf{1} = \sum_{i=0}^{n} e_i$ be the resolution of $\mathbf{1}$ corresponding to (25); $e_i \in U_i$, $U_i = e_i R^{\#}$. If U_o was decomposable, the idempotent e_o could be written as the sum $e_o = \varepsilon_1 + \varepsilon_2$ of two orthogonal idempotents $\varepsilon_1, \varepsilon_2 \in U_o$. Set $\varepsilon_1 = \rho_1 + m_1 \mathbf{1}$, $\varepsilon_2 = \rho_2 + m_2 \mathbf{1}$ with $\rho_1, \rho_2 \in R$; $m_1, m_2 \in \mathbb{Z}$. It follows from $\varepsilon_1 \varepsilon_2 = 0$ that $m_1 m_2 = 0$. Hence one of the m_j is 0 , say $m_1 = 0$. Then $\varepsilon_1 = \rho_1 \in R$ and the idempotent ε_1 would belong to the nilpotent r-ideal $U_o \cap R \subseteq \mathrm{Rad}(R)$. This is impossible.

(S**) If the assumptions and the notation are the same as in (S),

$$(28) \qquad R = (U_o \cap R) \dotplus U_1 \dotplus U_2 \dotplus \ldots \dotplus U_n .$$

Here, $U_o \cap R = (0)$, iff R has the left unit element e.

Proof. The equation (28) follows at once from (S). Let $1 = \sum_{i=0}^{n} e_i$ be the resolution of 1 belonging to (25) with $e_i \in U_i$. If $U_o \cap R = (0)$, it is seen at once that $e = 1 - e_o$ is a left unit element of R. Conversely, if R has a left unit element e, then, since $e_o e \in e_o R \subseteq R$, $e e_o e = e_o e$ and $(e_o e)^2 = (e_o e)$. As $e_o e \in U_o \cap R \subseteq \mathrm{Rad}\,(R)$, $e_o e$ cannot be an idempotent, we must have $e_o e = 0$. For $\rho \in U_o$, we have $\rho = e_o \rho$. If ρ also belongs to R, then $e\rho = \rho$ and hence $\rho = e_o \rho = e_o e \rho = 0$. Thus, $U_o \cap R = (0)$ as we wished to show.

(T) COROLLARY.* A semisimple m-ring R has a unit element.

Proof. Here, $U_o \cap R \subseteq \mathrm{Rad}\,(R) = (0)$ and, by (S*), R has a left unit element e. If $\alpha, \rho \in R$, then $(\alpha - \alpha e)\rho = \alpha\rho - \alpha\rho = 0$ whence $(\alpha - \alpha e)R = (0)$. Now, by Chapter III, (A), $\alpha - \alpha e \in \mathrm{Rad}\,(R)$, that is, $\alpha - \alpha e = 0$. Thus, e is a unit element.

---

* A direct proof of (T) is suggested in Problem 10 of Chapter III.

The theorems (L), (M), (N), (O) remain true for indecomposable components $U \subseteq R$ of $R^{\#}$. It is now clear that these U are exactly the minimal potent r-ideals of R. Stated explicitly, we have

(U) Let R be an m-ring. Each minimal potent r-ideal U of R has the greatest proper submodule $W = U \cap \text{Rad}(R)$. If U^* is a second minimal potent r-ideal and $W^* = U^* \cap \text{Rad}(R)$, then U and U^* are R-isomorphic, iff U/W and U^*/W^* are R-isomorphic.

Proof. Since U is minimal potent, $W = U \cap \text{Rad}(R) \neq U$ and every proper submodule Y of U is included in Rad (R) and hence in W. The last part is obtained by the proof of (N), see the Remark on p.95.

(V) Let R be an m-ring. If X is a minimal potent r-ideal of R and if $R = {}^{\bullet}\sum U_i$ is a full decomposition of $R^{\#}$ as in (S), then X is R-isomorphic to some $U_i \subseteq R$.

(W) Let R be an m-ring and let $X_1, X_2, \ldots, X_k$ be a system of minimal potent r-ideals of R such that each minimal potent r-ideal U of R is R-isomorphic with exactly one X_i. Then R has exactly k "distinct" irreducible representations $\tilde{f}_1, \tilde{f}_2, \ldots, \tilde{f}_k$ and the module of $\tilde{f}_i$ can be taken as X_i/Y_i with $Y_i = X_i \cap \text{Rad}(R)$.

These statements are obtained by the methods used in proving (M) and (O). It will not be necessary to give details. We only remark that the height of an m-ring R will be defined as the number k appearing in (W). For rings with 1, this coincides with the old definition.

6. Some further results.

(X) Let R be an m-ring with 1. Let U and U* be two indecomposable components of R. Then U and U* are R-isomorphic, iff $UU^* \not\subseteq \mathrm{Rad}(R)$.

Proof. By (F), Hom (U*, U) consists of the mappings

$$\theta: \quad u^* \to u_0 u^* , \qquad (u^* \in U^*) ,$$

where u_0 is a fixed element of U. If $UU^* \subseteq \mathrm{Rad}(R)$, each such θ maps U* into $UU^* \subseteq U \cap \mathrm{Rad}(R) \subset U$ and we cannot even have an R-homomorphism of U* onto U. If $UU^* \not\subseteq \mathrm{Rad}(R)$, we may choose $u_0 \in U$ such that $u_0 U^* \not\subseteq \mathrm{Rad}(R)$. Then the submodule $u_0 U^*$ of U is not included in the greatest proper submodule $U \cap \mathrm{Rad}(R)$ and hence $u_0 U^* = U$. Since θ maps U* onto $u_0 U^* = U$, it follows from (I*) that θ is an R-isomorphism of U* onto U.

(Y) THEOREM(Frobenius-Schur). Let R be an m-ring with 1 and let $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_k$ denote the "distinct" irreducible representations of R. Given k elements $\alpha_1, \alpha_2, \dots, \alpha_k$ of R, we can find an element ξ of R such that

$$(29) \qquad \mathcal{F}_1(\xi) = \mathcal{F}_1(\alpha_1),\ \mathcal{F}_2(\xi) = \mathcal{F}_2(\alpha_2),\ \dots,\ \mathcal{F}_k(\xi) = \mathcal{F}_k(\alpha_k) .$$

Proof. It will be sufficient to find elements $\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_k$ such that $\mathcal{F}_i(\mathcal{E}_i) = I$ and $\mathcal{F}_i(\mathcal{E}_j) = \square$ for $i \neq j$. Indeed, then $\xi = \sum_i \mathcal{E}_i \alpha_i$ satisfies (29).

Let $R = {}^{\bullet}\sum_i U_i$ be a full decomposition of R. Change now the notation denoting R-isomorphic components with the same subscript and distinguishing them by superscripts. Then our decomposition appears in the form

$$(30) \qquad R = {}^{\bullet}\sum_{i=1}^{k} {}^{\bullet}\sum_{\lambda=1}^{q_i} U_i^{(\lambda)} ,$$

where each $U_i^{(\lambda)}$ is indecomposable and where $U_i^{(\lambda)} \approx U_j^{(\mu)}$ iff $i = j$. It follows from (M) that each indecomposable component U of R is R-isomorphic to exactly one of the $U_i^{(1)}$, ($i=1, 2, \dots, k$) so that k is the height of R. Furthermore, if $W_i^{(1)} = U_i^{(1)} \cap \mathrm{Rad}(R)$, then the k simple modules $F_i = U_i^{(1)}/W_i^{(1)}$ belong to k "distinct" irreducible representations, cf. (N). Hence $\mathcal{F}_i$ may be taken as the representation in F_i .

Set $H_j = \cdot\sum_\lambda U_j^{(\lambda)}$ so that we have $R = \cdot\sum_{j=1}^k H_j$ and let $1 = \sum_{j=1}^k \mathcal{E}_j$ be the corresponding resolution of 1 . For $i \neq j$, the modules $U_i^{(1)}$ and $U_j^{(\lambda)}$ are not R-isomorphic and $(\underline{X})$ shows that $U_i^{(1)} U_j^{(\lambda)} \subseteq U_i^{(1)} \cap \operatorname{Rad}(R) = W_i^{(1)}$. Hence $U_i^{(1)} H_j = \sum_\lambda U_i^{(1)} U_j^{(\lambda)} \subseteq W_i^{(1)}$. In particular, $U_i^{(1)} \mathcal{E}_j \subseteq W_i^{(1)}$ for $i \neq j$ and as $\mathfrak{f}_i$ is the representation in $U_i^{(1)}/W_i^{(1)}$, $\mathfrak{f}_i(\mathcal{E}_j) = \square$ for $i \neq j$, cf. Chapter II, $(\underline{E})$. Furthermore

$$I = \mathfrak{f}_i(1) = \sum_{j=1}^k \mathfrak{f}_i(\mathcal{E}_j) = \mathfrak{f}_i(\mathcal{E}_i) .$$

Thus, $\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_k$ satisfy the required conditions.

The following proposition gives information about the structure of the additive group Hom (U, V) where U is an indecomposable component of R and V an R-module satisfying a "finiteness" condition. We shall use this in a later chapter.

$(\underline{Z})$ Let R be a ring with 1 . Let U be a projective R-module which has a greatest proper submodule W . Assume that V is an R-module which has a composition series

$$(31) \qquad V = V_0 \supset V_1 \supset V_2 \supset \ldots \supset V_{r-1} \supset V_r = (0) .$$

If exactly m of the quotients V_{i-1}/V_i are R-isomorphic with the simple module $F = U/W$, then the group $G = \mathrm{Hom}\,(U, V)$ has the normal series

$$G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_m = (0)$$

of length m such that all quotients G_{i-1}/G_i are isomorphic with the additive group $\mathcal{E}(F)^+$ of the skew field $\mathcal{E}(F)$.

Proof. Since F is a simple module, $\mathcal{E}(F)$ is a skew field, cf. (B).

We use induction on the length r of the composition series (31) of V. If $r = 0$, $V = (0)$ and (Z) is trivial.

If $r \geqq 1$, we may assume that (Z) holds for V_1 instead of V, since V_1 has the composition series $V_1 \supset V_2 \supset \dots \supset V_r = (0)$ of length $r - 1$. If m' of the quotients V_{i-1}/V_i with $i > 1$ are R-isomorphic with F, then $H = \mathrm{Hom}\,(U, V_1)$ has a normal series of length m' such that all its quotient groups are isomorphic with $\mathcal{E}(F)^+$. By (H),

$$G/H = \mathrm{Hom}\,(U, V)/\mathrm{Hom}\,(U, V_1) \approx \mathrm{Hom}\,(U, V/V_1) .$$

Since V/V_1 is a simple module, (C) yields $\mathrm{Hom}\,(U, V/V_1) \approx \mathrm{Hom}\,(U/W, V/V_1)$ and we have

$$G/H \approx \mathrm{Hom}\ (F,\ V/V_1)\ . \tag{32}$$

If V/V_1 is R-isomorphic with F, then $m = m' + 1$. Replacing V/V_1 by the isomorphic module F in (32), we see that $G/H \approx \mathrm{Hom}\ (F,\ F) = \mathcal{E}(F)^+$.

On the other hand, if V/V_1 is not R-isomorphic with F, then $m = m'$. Here ($\underline{A}$) implies $\mathrm{Hom}\ (F,\ V/V_1) = (\square)$ and then (32) shows that $G = H$.

In either case, the statement ($\underline{Z}$) for $G = \mathrm{Hom}\ (U,\ V)$ is an immediate consequence of the corresponding statement for $H = \mathrm{Hom}\ (U,\ V_1)$.

Problems to Chapter IV

For definition of the concepts: "Completely reducible group"; "Cartesian direct sum and product of a system of groups"; "Exact sequence of groups", consult the appendix. We consider there the case that we have groups with a fixed system of operators. In particular, we may take R-modules with a fixed ring R .

The following definitions are also used. In all of them, R denotes a ring with unit element 1 .

DEFINITIONS.

1. A free R-module T is a module which is a direct sum of submodules R_i which are R-isomorphic with $R^{\cdot}$. If a fixed R-isomorphism of $R^{\cdot}$ onto R_i maps $1 \rightarrow t_i$, the set $\{t_i\}$ is called an R-basis of T . The most general element of T can be written uniquely in the form $\sum_i t_i \alpha_i$ such that $\alpha_i \in R$ and that only finitely many α_1 are different from 0 .

2. An R-module V is injective (H. Cartan-S. Eilenberg, Homological Algebra, p. 8), if it has the following property: If A is any R-module, B a submodule, θ an R-homomorphism of B into V , then θ can be extended to an R-homomorphism of A into V .

3. Let V be an R-module. A Loewy series is a finite set of submodules $V_1 \subset V_2 \subset \dots \subset V_n$ such that each quotient V_{i+1}/V_i is completely reducible $(i = 1, 2, \dots, n-1)$.

Note. In order to avoid repetition, the assumptions concerning the rings R are stated at the beginning of each section. If R is a ring with unit element $\mathbb{1}$, it is assumed that all R-modules considered are unitary, i.e., that we have $v\mathbb{1} = v$ for all elements v of modules.

I. Problems for arbitrary rings with unit element.

In problems 1 - 11, the ring R is assumed to be a ring with unit element. All modules are assumed to be unitary.

1. If R is a direct sum $R = {}^{\bullet}\sum_i U_i$ of components, the number of components U_i is necessarily finite.

2. Let $R = {}^{\bullet}\sum_{i=1}^{n} U_i$ be a decomposition of R into components and let $\mathbb{1} = \sum_{i=1}^{n} e_i$ be the corresponding resolution of $\mathbb{1}$. Show that $U_1, U_2, \dots, U_n$ are ideals of R, iff $e_1, e_2, \dots, e_n$ belong to the center C of R. Obtain a one-to-one correspondence between decompositions of R and of C into ideals.

3. Show that every R-module V is an R-homomorphic image of a free module T. Show further that if the ascending chain

condition holds for submodules of V , then T may be chosen as a free module with a finite basis.

4. Let P be a projective module and let

$$A \xrightarrow{\theta} B \xrightarrow{\eta} C$$

be an exact sequence of R-modules. Define mappings θ^*, η^*, depending on θ, η in a natural manner such that

$$\mathrm{Hom}\,(P,\ A) \xrightarrow{\theta^*} \mathrm{Hom}\,(P,\ B) \xrightarrow{\eta^*} \mathrm{Hom}\,(P,\ C)$$

is an exact sequence of groups .

5. (a) Let X and Y be two R-modules and let Z be a common submodule of both. Construct an R-module G with the following properties: 1) X is a submodule of G . 2) There exists an R-isomorphism ω of Y into G which leaves every element of Z fixed.

(b) Use (a) for a proof of the following proposition: Suppose a module Q has the property that whenever Q is a submodule of a module G , then G is the direct sum $G = Q \dot{+} T$ of Q and another submodule. Then Q is injective.

(c) Prove also the converse of (b): If an injective module Q is a submodule of a module G, then G is a direct sum of Q and another submodule.

Hint: It is natural to take G in (a) as a homomorphic image of $X \oplus Y$.

6. Assume that an R-module P has the property that whenever θ is an R-homomorphism of an R-module V onto P, then V is the direct sum of the kernel of θ and another submodule. Show that P is projective. (Converse of (I).)

7. Let R be the ring of all matrices

$$\alpha = (a_{ij}), \quad (i, j = 1, 2, \ldots, n)$$

of a fixed degree n with coefficients a_{ij} in a given skew field S. For each h with $1 \leq h \leq n$, let U_h denote the r-ideal consisting of the $\alpha = (a_{ij})$ with $a_{ij} = 0$ for $i \neq h$. Find all idempotents in U_h. Show further that $R = \cdot\sum_{h=1}^{n} U_h$ is a full decomposition of R and give the corresponding resolution of 1.

8. Let R be the ring of all triangular matrices

$$\alpha = \begin{bmatrix} a_{11} & 0 & 0 & \dots \\ a_{21} & a_{22} & 0 & \dots \\ a_{31} & a_{32} & a_{33} & \dots \\ \dots & \dots & \dots & \dots \end{bmatrix}$$

with a countable infinite number of rows and columns and with coefficients in a given skew field; $a_{ij} = 0$ for $i < j$. Let U_h be the r-ideal consisting of all $\alpha \in R$ with $a_{ij} = 0$ for $i \neq h$.

(a) Show that each U_h is an indecomposable component of R, but that $\dot{\sum}_{h=1}^{\infty} U_h$ is a proper subring of R.

(b) Show that the m-condition holds for submodules of U_h. What is the greatest proper submodule of U_h?

(c) Show that R is not an m-ring in each of the following ways 1) by constructing a strictly descending infinite chain of r-ideals; 2) by showing that Rad (R) is not nilpotent; 3) by showing that R cannot be written as a direct sum of indecomposable components.

9. Let $R = \mathbb{Z}$ be the ring of rational integers. Give an example of an indecomposable R-module which does not have maximal submodules.

10. (a) Let $\hat{R}$ be the additive group of all characters χ of the additive group R^+ of R, i.e., of all additive homomorphisms χ of R into the additive group of real numbers modulo 1. The image of $\alpha \in R$ under χ will here be denoted by $\chi(\alpha)$. For $\chi \in \hat{R}$, $\rho \in R$, define $\chi\rho$ by $(\chi\rho)(\alpha) = \chi(\rho\alpha)$ for $\alpha \in R$. Show that $\hat{R}$ is an injective module.

(b) Show that each R-module A is R-isomorphic with a submodule of a Cartesian direct product Q_A of "sufficiently many" equal factors $\hat{R}$. Note that Q_A is an injective module. Hence A is a submodule of an injective module.

Remark. More generally, $\hat{R}$ can be taken as any group of the form Hom (R^+, T) where T is an abelian group with the following properties: 1) T is divisible, i.e., for every natural integer n and every $t \in T$, there exist elements $s \in T$ with $ns = t$. 2) For every natural integer n, there exist elements of order n in T.

Hints. Full use should be made of Zorn's lemma or of equivalent principles. Observe the following properties of abelian groups G. A character of a subgroup H of G can be extended to a character of G. It follows that if $g \in G$, $g \neq 0$, there exist characters χ of G with $\chi(g) \not\equiv 0 \pmod 1$. This implies that if H is a subgroup of G and $g \in G$, $g \notin H$, there exist characters

χ of G with $\chi(g) \not\equiv 0 \pmod 1$, $\chi(h) \equiv 0 \pmod 1$ for all $h \in H$. Analogous statements can be made, if $\hat{R} = \mathrm{Hom}(R^+, T)$ as in the "Remark". In answering (b), it may be helpful to think first of the case that $A = aR$ with $a \in A$. Find an element $q \in Q_A$ for suitable choice of Q_A such that the mapping $a\rho \to q\rho$ for $\rho \in R$ is a well-defined R-isomorphism of A.

In the general case, it is sufficient to take the set of indices in the Cartesian product as $A \times \hat{R}$.

11. There is a kind of duality between projective and injective modules. Explore this.

II. Problems for m-rings with unit elements.

In problems 12-22, R is assumed to be an m-ring with unit element. All modules are assumed to be unitary.

12. Let V be an R-module which has a greatest proper submodule. Show that V is an R-homomorphic image of an indecomposable component of R.

13. Let $V \neq (0)$ be an R-module. Show that V has both maximal and minimal submodules.

Hints. In proving the existence of minimal submodules, we may replace V by a submodule of the form $vR \neq (0)$ generated by one element v.

In order to prove the existence of maximal submodules, set $N = \mathrm{Rad}\,(R)$ and show first that $VN \neq V$. Let $1 = \sum e_i$ be a full resolution of 1. Choose $v \in V$, $v \notin VN$ such that $v = ve_j$ for some j. Use Zorn's lemma to construct a submodule Z such that $VN \subseteq Z \subset V$, $v \notin Z$, which is maximal with these properties. Show that Z is maximal in V.

14. Let V be an R-module which satisfies the ascending chain condition for submodules. Apply #3 (and some group theory) to show that the descending chain condition for submodules of V holds.

15. Let V be a projective module which satisfies the ascending chain condition for submodules. Show that V is a direct sum of a finite number of submodules each of which is R-isomorphic with an indecomposable component of R.

16. Let U and U* be two indecomposable components of R, let $\mathcal{U}$ and $\mathcal{U}^*$ denote the corresponding indecomposable representations, and let $\mathcal{F}$ be the unique irreducible quotient representation

of $\mathscr{U}$ (belonging to the module $F = U/(U \cap \operatorname{Rad} R)$). Show that $U^*U \neq (0)$, iff $\mathscr{F}$ appears as a constituent of $\mathscr{U}^*$ (i.e., iff U^* has submodules $X \supset Y$ with $X/Y \approx F$).

17. Let $R = {}^{\bullet}\sum_{i=1}^{n} U_i$ be a full decomposition of R. Distribute $U_1, U_2, \ldots, U_n$ into sets $B_1, B_2, \ldots, B_t$ such that U_α and U_β belong to the same set B_j, iff there exists a finite sequence

$$U_{i_0} = U_\alpha, \; U_{i_1}, \ldots, U_{i_r} = U_\beta$$

with $1 \leqq i_0, i_1, \ldots, i_r \leqq n$ such that, for each $\rho = 1, 2, \ldots, r$, at least one of the products $U_{i_\rho} U_{i_{\rho-1}}$, $U_{i_{\rho-1}} \cdot U_{i_\rho}$ is not (0). Let H_j be the sum of the $U_i \in B_j$.

(a) Show that $H_1, H_2, \ldots, H_t$ are ideals.

(b) Show that if R is written as a direct sum $R = {}^{\bullet}\sum A_\lambda$ of ideals A_λ, each A_λ is a direct sum of some of the H_j, with each H_j appearing in exactly one A_λ. Deduce that no H_j can be written as a direct sum of two ideals $\neq (0)$ and that $R = {}^{\bullet}\sum_{j=1}^{t} H_j$ is the only decomposition of R into ideals $\neq (0)$ with this property. The ideals H_j are called the block ideals of R.

18. (Continuation of #17). Let $\mathfrak{U}_i$ be the representation belonging to U_i. Use #16 to show that U_α and U_β belong to the same set B_j, iff there exists a finite sequence

$$\mathfrak{U}_{k_0} = \mathfrak{U}_\alpha, \mathfrak{U}_{k_1}, \ldots, \mathfrak{U}_{k_s} = \mathfrak{U}_\beta$$

such that $\mathfrak{U}_{k_{\sigma-1}}$ and $\mathfrak{U}_{k_\sigma}$ have a common irreducible constituent; $(1 \leqq k_\nu \leqq n)$.

19. Let V be an R-module. Set $L_0(V) = (0)$. If $L_r(V)$ is already defined for some r and if $L_r(V) \neq V$, let $L_{r+1}(V)$ be the sum of all submodules $X \supset L_r(V)$ such that $X/L_r(V)$ is simple. If $L_r(V) = V$, let $L_{r+1}(V) = V$.

(a) Show that $L_{r+1}(V)/L_r(V)$ is completely reducible if $L_r(V) \neq V$.

(b) If $A_0 = (0) \subset A_1 \subset A_2 \subset \ldots \subset A_r$ is a Loewy series, show that $A_r \subseteq L_r(V)$.

(c) If Z is a submodule of V, show that $L_r(Z) = Z \cap L_r(V)$.

(d) Let $N = \mathrm{Rad}\,(R)$ and set $N^0 = R$. Prove that $L_r(R^{\cdot}) = \{ \rho \mid \rho N^r = (0), \rho \in R \}$ for $r = 0, 1, 2, \ldots$

(e) If V is an R-module, show that $V\, L_r(R^\cdot) \subseteq L_r(V)$. Give examples which show that the equality sign does not always hold.

Let h be the smallest exponent for which $N^h = (0)$. If V is an R-module, it follows from (d) and (e) that there exist integers s with $0 \leq s \leq h$ such that $L_s(V) = V$. The smallest s possible here is called the Loewy length $s = \lambda(V) = V$; the series $(0) \subset L_1(V) \subset L_2(V) \subset \ldots \subset L_s(V) = V$ is the lower Loewy series of V and $L_1(V)$ is the socle of V.

Hints. (a) Use Zorn's lemma to show that $L_1(V)$ is a direct sum of simple modules. Apply this to $V/L_r(V)$. (d) Show $L_r(R^\cdot)N \subseteq L_{r-1}(R^\cdot)$ and deduce $L_r(R^\cdot)\, N^r = (0)$. In order to show that $\xi N^r = (0)$ for $\xi \in R$ implies $\xi \in L_r(R^\cdot)$, use induction on r. Let $1 = \sum e_i$ be the full resolution of 1. Show that for each i, the module $\xi e_i R + L_{r-1}(R^\cdot)$ is either $L_{r-1}(R^\cdot)$ or a module minimal over $L_{r-1}(R^\cdot)$ and deduce $\xi \in L_r(R^\cdot)$. (e) If $v \in V$, let θ be the homomorphism $\rho \rightarrow v\rho$ of $R^\cdot$ onto vR. Use (b) to obtain $L_r(R^\cdot)\,\theta \subseteq L_r(vR)$ and then apply (c).

20. Let V be an R-module. If $V \neq (0)$, the upper cover $L^{(1)}(V)$ of V is the intersection of the maximal submodules of V, (cf. #13). For $V = (0)$, set $L^{(1)}(V) = (0)$. Define recursively $L^{r+1}(V) \doteq L^{(1)}(L^{(r)}(V))$, $r = 1, 2, \ldots$.

(a) Show that $L^{(r)}(V)/L^{(r+1)}(V)$ is completely reducible (if $L^{(r)}(V) \neq (0)$).

(b) If $s = \lambda(V)$ is the Loewy length of V (cf.#19), show that

$$V = L^{(0)}(V) \supset L^{(1)}(V) \supset \ldots \supset L^{(s-1)}(V) \supset L^{(s)}(V) = (0) .$$

This is the upper Loewy series of V.

(c) If $N = \text{Rad}(R)$, show $L^{(j)}(R^{\cdot}) = N^j$ for $j = 0, 1, 2, \ldots$.

(d) If V is an R-module of Loewy length $\lambda(V) = s$, show that $L^{(j)}(V) \subseteq L_{s-j}(V)$, $L^{(j)}(V) \not\subseteq L_{s-j-1}(V)$ for $j = 0, 1, 2, \ldots, s-1$. Show further that there exist simple R-modules ($\neq (0)$) which are R-isomorphic to submodules of both $L^{(j)}(V)/L^{(j+1)}(V)$ and $L_{s-j}(V)/L_{s-j-1}(V)$; $(0 \leqq j \leqq s-1)$.

Hints. Note that if W is a submodule of V, then $L^{(1)}(W) \subseteq L^{(1)}(V)$. The crucial point is to show that if $L^{(1)}(V) = (0)$, then V is completely reducible. If this was not so, then by #19 there exist $v \in V$ such that vR is not completely reducible while, by the first remark, $L^{(1)}(vR) = (0)$. Now $vR \approx R^{\cdot}/X$ where X is an r-ideal of R. Then (0) is the intersection of a finite number of simple submodules of vR and this implies that vR is completely reducible.

(b) Prove that if V is an R-module and $s = \lambda(V)$, then $L^{(1)}(V) \subseteq L_{s-1}(V)$. Apply this to various modules to obtain $L^{(r)}(V) \subseteq L_{s-r}(V)$. If $L^{(t)}(V) = (0)$ for $t < s$, apply #19(b) to $L^{(t)}(V) \subset L^{(t+1)}(V) \subset \ldots$ to obtain a contradiction.

(c) Show $L^{(r-1)}(R^{\cdot}) N \subseteq L^{(r)}(R^{\cdot})$ and deduce $N^r \subseteq L^{(r)}(R^{\cdot})$. In order to prove the reverse inequality, show that N^{r-1}/N^r is completely reducible. Observe that N^{r-1}/N^r may be considered as an R/N-module and here the preceding results of #19, #20 apply with $h = 1$.

21. Let P be a projective R-module. Show that P is a direct sum of modules R-isomorphic with indecomposable components of R. (This extends #15.)

Hints. Let $N = \mathrm{Rad}(R)$. Then P/PN is an R/N-module and, by #19, it is a direct sum of simple modules. Construct a homomorphism of P onto a module A/B where A is a Cartesian sum $A = \oplus \sum X_i$ of indecomposable components X_i of R and $B = \oplus \sum (X_i \cap N)$. Using the projectivity of P, find a homomorphism φ of P into A and show that $P\varphi$ is of the same type as A and that the kernel L of φ is included in PN. Obtain $P = P_1 \dotplus L$ with $P_1 \approx P\varphi$. Apply the same argument to L, etc.

22. (a) Let H be a module which has only one simple submodule F and assume that every module $H_1 \supset H$ has simple submodules different from F. Show that H is injective.

(b) If F is a simple module, show that there exists an injective module H_F with F as its only simple submodule. Show also that H_F is uniquely determined up to R-isomorphism.

(c) Show that if Q is an injective R-module, then Q is R-isomorphic to a Cartesian direct product of factors of the form H_F.

(d) Compare #22 and #21 in the sense of #11.

Hints. (a) Let W be a module with $W \supset H$. Construct a maximal submodule Y with $Y \cap H = (0)$. Show that $W = Y \dotplus H$ by assuming that there exists a submodule $W_0 \supset Y \dotplus H$ of W which is minimal over $Y \dotplus H$, and obtaining a contradiction. Now apply #5.

(b) We have to show the existence of a module H with the properties assumed in (a). First method: Let Q be an injective module including F, cf. #10 and choose H as a maximal submodule of Q which includes F as only simple submodule. Second method: Apply Zorn's lemma directly (with sufficient care!).

III. Problems for arbitrary m-rings.

In problems 23-26, it is assumed that R is an m-ring but not that R has a unit element. As always, $R^\#$ denotes the extended ring with unit element $\mathbb{1}$.

23. Show that if $R^\#$ is written as a direct sum of components, all but one of the components lie in R. (This does not depend on the m-condition.

24. Show that every r-ideal A of R can be written as a direct sum $A = A_o \dot{+} A_1 \dot{+} \dots \dot{+} A_n$ such that 1) $A_o \subseteq \mathrm{Rad}\,(R)$ 2) $A_1, A_2, \dots, A_n$ are minimal potent r-ideals 3) The sum $A_1 \dot{+} A_2 \dot{+} \dots \dot{+} A_n$ is a component of $R^\#$ (except when $A \subseteq \mathrm{Rad}\,(R)$ in which case $n = 0$ and $A_1, \dots, A_n$ are missing).

25. Give a proof of $(\underline{S})$, $(\underline{S}^*)$ using the methods of § 4.

Suggested procedure: Show that R can be written as a direct sum $R^\# = U_o \dot{+} B$ of r-ideals such that 1) $B \subseteq R$, 2) If U^*_o is a submodule of U_o, either $U^*_o + B^* \neq R^\#$ for every r-ideal B^* of R or $U_o \cap R = U^*_o \cap R$. Prove that then U_o is indecomposable and that it cannot be written as a sum $X + Y$ of two r-ideals with $X \subset U_o$, $Y \subseteq R$. Deduce that $U_o \cap R \subset \mathrm{Rad}\,(R)$ and finish up.

26. Prove $(\underline{V})$ and $(\underline{W})$.

IV. A supplement.

The results of § 5 hold for a class of rings R slightly more general than m-rings.

27. Assume that R is a ring which possesses a nil ideal N such that R/N is a semisimple m-ring. Call an r-ideal X potent, if it is not a nil-r-ideal.

(a) Show that $N = \mathrm{Rad}(R)$, that every potent r-ideal X contains idempotents, and that every potent r-ideal includes minimal potent r-ideals.

(b) Check that the results of § 5 holds for R .

Rings R satisfying the assumptions of #27 are sometimes called semi-primary rings (cf. Deuring, Algebren, Erg. der Math., vol. 4).

Hints. If X is an r-ideal of R , then $(X+N)/N$ is an r-ideal of the semisimple m-ring $R^* = R/N$. If X is potent, it follows that it contains elements η with $\eta^2 \equiv \eta \not\equiv 0 \pmod{N}$ and now an idempotent e of X can be constructed as in the proof of (Q). In (b), the methods of § 5 can be used without change except that in the proof of (S), it has to be shown that the process terminates after a finite number of steps.

CHAPTER V

THE STRUCTURE OF SEMISIMPLE m-RINGS

If R is an m-ring (Chapter III, § 8), we know that $N = \text{Rad}(R)$ is nilpotent and that $R^* = R/N$ is semisimple. Since a homomorphic image of an m-ring is an m-ring, the problem of constructing all m-rings can be reduced to the following three problems:

(I) Construct all semisimple m-rings R^*.

(II) Construct all nilpotent rings N.

(III) Given a semisimple m-ring R^* and a nilpotent ring N, solve the extension problem of finding all m-rings R with $\text{Rad}(R) = N$ such that $R/N \approx R^*$.

In this chapter, we discuss Problem (I). This is the Wedderburn structure theory (developed by Wedderburn for finite dimensional algebras). Not much is known about Problem (II). A result of Wedderburn concerning Problem (III) requires stronger assumptions and will be dealt with later.

REMARKS.

1. The results of this chapter (except those of the last section) are special cases of those of Chapter VI.

2. If we are only interested in the Wedderburn structure theorems, more direct proofs are available, see for instance Problems 5 and 7.

3. The second Wedderburn theorem is a special case of Jacobson's density theorem (Part 2, Ch. I) which provides a very

simple approach to this theorem.

4. A similar program as that stated for m-rings could be proposed for arbitrary rings. We would have to construct all semi-simple rings and all radical rings and we would have to solve an extension problem. No satisfactory results are available in the general case.

1. Cartesian direct sum of rings.

In the appendix § 7, the Cartesian direct sum of groups is defined, An analogous definition can be given in the case of rings, and the results are quite analogous.

Let $R_1, R_2, \ldots, R_n$ be n given rings. Let S be the set of all n-tuples

$$(1) \qquad s = (r_1, r_2, \ldots, r_n)$$

with $r_1 \in R_1$, $r_2 \in R_2, \ldots, r_n \in R_n$. Define addition and multiplication by the formulas

$$(2) \qquad (r_1, r_2, \ldots, r_n) + (\rho_1, \rho_2, \ldots, \rho_n) = (r_1 + \rho_1, r_2 + \rho_2, \ldots, r_n + \rho_n),$$

$$(3) \qquad (r_1, r_2, \ldots, r_n)(\rho_1, \rho_2, \ldots, \rho_n) = (r_1\rho_1, r_2\rho_2, \ldots, r_n\rho_n)$$

(where of course $\rho_1 \in R_1$, $\rho_2 \in R_2, \ldots, \rho_n \in R_n$). It is obvious that then S becomes a ring, the Cartesian direct sum

$$S = R_1 \oplus R_2 \oplus \cdots \oplus R_n = \oplus \sum_{\alpha=1}^{n} R_\alpha$$

of the rings R_α.

Let α be a fixed index, $1 \leqq \alpha \leqq n$ and let i_α denote the mapping of $R_\alpha \longrightarrow S$ defined by

$$(4) \qquad r_\alpha \longrightarrow (0, \ldots, 0, r_\alpha, 0, \ldots, 0)$$

where the term $r_\alpha \in R_\alpha$ stands at the α-th place. Clearly, i_α is a ring isomorphism, the α-th injection. It is also obvious that the image $R_\alpha i_\alpha = \tilde{R}_\alpha$ is an ideal of S and that S is the direct sum of these ideals:

$$(5) \qquad \oplus \sum_{\alpha=1}^{n} R_\alpha = \cdot \sum_{\alpha=1}^{n} \tilde{R}_\alpha \; ; \; R_\alpha \approx \tilde{R}_\alpha$$

Conversely, assume that a ring R is written as a direct sum $R = \cdot \sum_{\alpha=1}^{n} R_\alpha$ of n ideals R_α. Each ideal R_α is of course a ring. Since the sum is direct, $R_\alpha \cap R_\beta = (0)$ for $\alpha \neq \beta$ and since $R_\alpha R_\beta \subseteq R_\alpha \cap R_\beta$ (as R_β is an ℓ - ideal and R_α an r-ideal), we have

$$(6) \qquad R_\alpha R_\beta = (0), \qquad \text{for } \alpha \neq \beta .$$

Every element $r \in R$ has a unique representation $r = \sum_{\alpha=1}^{n} r_\alpha$ with $r_\alpha \in R$. If we map

$$r \longrightarrow (r_1, r_2, \ldots, r_n)$$

then we see easily using (6) that we have a ring isomorphism θ of R onto $\oplus \sum_{\alpha=1}^{n} R_\alpha$;

$$(7) \qquad \cdot \sum_{\alpha=1}^{n} R_\alpha \approx \oplus \sum_{\alpha=1}^{n} R_\alpha .$$

Because of (5) and (7), we usually don't distinguish carefully between "direct sums" of ideals and "Cartesian direct sums" of rings.

However, in principle, they are not the same thing. In a direct sum we have a given ring R and the R_α are ideals of R. In a Cartesian direct sum, we start from arbitrary rings R_α and create a new ring S. Here, even all the R_α may be equal.

If α is fixed, $1 \leqq \alpha \leqq m$, the mapping

$$(8) \qquad (\rho_1, \rho_2, \dots, \rho_n) \longrightarrow \rho_\alpha$$

is a ring homomorphism p_α of $\oplus \Sigma R_\alpha$ onto R_α, the α-th projection. As in the case of groups,

$$(9) \qquad \begin{cases} i_\alpha p_\alpha = I_\alpha \; ; \; i_\alpha p_\beta = \Box_\alpha & \text{for } \alpha \neq \beta \\ \sum\limits_\alpha p_\alpha i_\alpha = I & \end{cases}$$

where I_α is the identity map of R_α, I is the identity map of $\oplus \sum\limits_\alpha R_\alpha$ and $\Box_\alpha$ is the zero-map of R_α.

The zero-element of $\oplus \sum_\alpha R_\alpha$ is obtained by taking each r_α in (1) as the zero-element 0 of R_α. If each R_α has a unit element 1_α, then $\oplus \sum_{\alpha=1}^{n} R_\alpha$ has a unit element obtained by taking each $r_\alpha = 1_\alpha$ in (1).

There is no difficulty about defining the Cartesian direct sum of infinitely many rings R_i. We consider here collections $\{r_i\}$ such that, for each index i, we have an element $r_i \in R_i$ such that only finitely many r_i are different from 0. Everything carries over, except the very last remark concerning the existence of a unit element.

2. Structure of semisimple m-rings.

Let R $\neq$ (0) be a semisimple m-ring. We know (Chapter IV, (T), also Chapter III, Problem 10) that R has a unit element 1. This saves us the trouble to require this as a separate assumption concerning R. By Chapter IV, (0), R has a finite number k of "distinct" irreducible representations $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_k$ and k is what we called the height of R. Each $\mathcal{F}_j$ is a ring homomorphism of R onto a certain ring consisting of all $\mathcal{F}_j(\rho)$ with $\rho \in R$. We shall denote this ring by $\{\mathcal{F}_j\}$,

$$\{\mathcal{F}_j\} = \{\mathcal{F}_j(\rho) \mid \rho \in R\}.$$

Clearly, $\{\mathcal{F}_j\}$ is a primitive ring in the sense of the following definition.

DEFINITION 1. A ring R is primitive, if R possesses faithful irreducible representations. (Neither the m-condition nor the existence of a unit element is required.)

Indeed, the identity map $\mathcal{F}_j(\rho) \longrightarrow \mathcal{F}_j(\rho)$ of $\{\mathcal{F}_j\}$ is a ring isomorphism $\tilde{\mathcal{F}}_j$ of $\{\mathcal{F}_j\}$ onto a set of endomorphisms of an abelian group and this representation $\tilde{\mathcal{F}}_j$ is irreducible, since the representation $\mathcal{F}_j$ of R was irreducible.

(A) If R $\neq$ (0) is a semisimple m-ring and if $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_k$ are the "distinct" irreducible representations of R, then the mapping θ

(10) $$\rho \longrightarrow (\mathcal{F}_1(\rho), \mathcal{F}_2(\rho), \ldots, \mathcal{F}_k(\rho))$$

is a ring isomorphism of R onto the Cartesian sum $\oplus \sum_{j=1}^{k} \{\mathcal{F}_j\}$ of the primitive rings $\{\mathcal{F}_j\}$.

Proof: It is clear that θ is a ring homomorphism of R into the Cartesian sum $\oplus \sum_{j=1}^{k} \{\mathcal{F}_j\}$. Actually, the Frobenius-Schur Theorem (Chapter IV, (Y)) shows that R is mapped onto the Cartesian sum. If ρ belongs to the kernel of θ, then $\mathcal{F}_j(\rho) = \square$ for $1 \leqq j \leqq k$. If $\mathcal{F}$ is any irreducible representation of R, $\mathcal{F}$ is equivalent to one of the $\mathcal{F}_j$ and hence $\mathcal{F}(\rho) = \square$. This shows that $\rho \in \mathrm{Rad}\,(R)$ and as R was semisimple, $\rho = 0$. Thus, θ is an isomorphism.

We now come to the definition of simple rings R. The essential requirement is that R has only the trivial ideals (0) and R. This is equivalent with saying that each ring homomorphism of R is either an isomorphism of R or the zero-mapping. This shows the analogy with the definition of simplicity in group theory.

If R has only the trivial ideals (0) and R, then in particular either Rad (R) = (0) or Rad(R) = R, that is, R is either semisimple or a radical ring. Since we want simple rings to be semisimple, we define now

DEFINITION 2. A ring R (with or without m-condition) is simple, if R has only the trivial ideals (0) and R, and if R is not a radical ring[*].

---

[*] The exclusion of radical rings in not completely standard and we reserve the right to change our attitude in later chapters. Of course, if we consider only rings with unit element, the whole point does not arise.

(B) A simple ring R is primitive. A primitive ring is semisimple.

Proof: 1) Since a simple ring R is not a radical ring, R has an irreducible representation $\mathfrak{F}$, (Chapter III, § 1). The kernel T of $\mathfrak{F}$ is an ideal of R and since we must have $T \neq R$, it follows that $T = (0)$. Hence $\mathfrak{F}$ is faithful and R is primitive.

2) If R is primitive and if $\mathfrak{F}$ is a faithful irreducible representation, then $\nu \in \operatorname{Rad}(R)$ implies $\mathfrak{F}(\nu) = \square$ and hence $\nu = 0$. Thus, $\operatorname{Rad}(R) = (0)$ and R is semisimple.

Primitive rings without m-condition will be discussed in a later chapter. They need not be simple. This is different if we assume the m-condition. Here, Definition 2 can be given in the following form:

DEFINITION 2*. An m-ring $R \neq (0)$ is *simple*, if R has only the trivial ideals (0) and R, and if R is not a ring consisting of a prime number of elements with $R^2 = (0)$.

Indeed, if R has only the trivial ideals, then the ideal R^2 must be either R or (0). In the former case, R is not nilpotent and hence not a radical ring. If $R^2 = (0)$, every additive subgroup of R is an ideal. Since the only such subgroups then are (0) and R, R must consist of a prime number of elements.

(C) Let R be a m-ring. The following three statements are equivalent:

(I) R is simple.

(II) R is primitive.

(III) R is semisimple of height $k = 1$.

Proof: By (B), (I) implies (II). Further, a primitive ring R is semisimple and hence (A) can be applied. We must have $k = 1$, since otherwise none of the "distinct" representations $\mathfrak{F}_1, \mathfrak{F}_2, \dots, \mathfrak{F}_k$ could be faithful. Finally, if R is semisimple and $k = 1$, then all irreducible representations are equivalent and hence have the same kernel M and then $M = \mathrm{Rad}(R) = (0)$. If R had an ideal $H \neq (0)$, R, an irreducible representation of R/H, would yield an irreducible representation of R with a kernel $\supseteq H$, a contradiction. Hence R is simple.

Combination of (A) and (C) yields

(D) First Wedderburn Theorem. A semisimple m-ring is isomorphic with a Cartesian sum $\oplus \Sigma_{j=1}^{k} R_j$ of simple rings R_j.

Indeed, every ring $\{\mathfrak{F}_j\}$ in (A) is a homomorphic image of an m-ring and hence an m-ring. Now, (C) shows that the primitive m-ring $R_j = \{\mathfrak{F}_j\}$ is simple.

3. The converse of the first structure theorem. Uniqueness.

LEMMA. Let $R = \oplus \sum_{j=1}^{k} R_j$ be a Cartesian sum of k rings R_j each of which has a unit element 1_j. Each r-ideal X of R has the form $X = \oplus \Sigma_j Y_j$ where Y_j is an r-ideal of R_j. Conversely, each such sum $\oplus \Sigma_j Y_j$ is an r-ideal of R.

Proof: Let $1 \leqq \alpha \leqq k$. The α-th projection p_α of $R = \oplus \Sigma_{j=1}^{k} R_j$ maps an r-ideal X of R onto an r-ideal Y_α of R_α. Let $\tilde{1}_\alpha$ be the image of 1_α under the α-th injection i_α, i.e., $\tilde{1}_\alpha$ is the element of R whose α-th "component" is 1_α while all other components vanish. Then $X\tilde{1}_\alpha \subseteq X$. Clearly, $X\tilde{1}_\alpha$ is the set $\tilde{Y}_\alpha$ obtained from Y_α by the injection i_α. Thus,

$$X = X1 = X \sum_{\alpha=1}^{k} \tilde{1}_\alpha = \cdot\sum_{\alpha=1}^{k} \tilde{Y}_\alpha = \oplus\sum_{\alpha=1}^{k} Y_\alpha .$$

The last statement of the lemma is obvious. It is also clear that X is an ideal of R, if each Y_j is an ideal of R_j.

In particular, if all R_j are m-rings, it follows from the lemma that $R = \oplus \Sigma_{j=1}^{k} R_j$ is an m-ring. Moreover, if each R_j is simple, the most general ideal of R has the form

(11) $$X = \oplus \Sigma Y_j \text{ , with } Y_j = (0) \text{ or } Y_j = R_j .$$

If some Y_j here is R_j, then X contains an idempotent $\tilde{1}_j$ and then $X \neq \text{Rad}(R)$. Hence Rad (R) = (0) and we have

(E) A Cartesian direct sum of finite number of simple m-rings is a semisimple m-ring.

The Lemma also yields the uniqueness theorem

(F) If R is a semisimple m-ring, there is a unique way in which R can be written as a direct sum of ideals which are simple rings.

Proof: Because of (D), we may take R in the form $R = \oplus \sum_{j=1}^{k} R_j$ where $R_1, R_2, \ldots, R_k$ are simple rings. The most general ideal X of R then has the form (11), and if X is to be a simple ring, exactly one of the Y_α must be R_α and all other Y_j must be (0). Let $\widetilde{R}_\alpha$ be the ideal X obtained in this manner. Then, $R = \bullet \sum_{\alpha=1}^{k} \widetilde{R}_\alpha$ and as $R_\alpha \approx \widetilde{R}_\alpha$, $\widetilde{R}_\alpha$ is a simple ring.

(F*) Corollary: The simple rings R_j in (D) are determined by R up to isomorphism.

4. Endomorphisms of Cartesian sums of abelian groups.

Before studying the structure of simple m-rings, we need a group theoretical lemma. We consider here a Cartesian sum $V = \oplus \sum_{j=1}^{q} V_j$ of abelain groups V_j which all have the same domain R of operators (cf. appendix, section 5). Let again i_α denote the α-th injection $V_\alpha \longrightarrow V$ and p_α the α-th projection $V \longrightarrow V_\alpha$. As in (9), we have

$$(12) \qquad \begin{cases} i_\alpha p_\alpha = I_\alpha ; \ i_\alpha p_\beta = \square_\alpha & \text{for } \alpha \neq \beta \\ \displaystyle\sum_{\alpha=1}^{q} p_\alpha i_\alpha = I . & \end{cases}$$

Let θ be an element of $\mathcal{E}(V)$, the ring of R-endomorphisms of V. If α and β are any two of the indices $1, 2, \ldots, k$, we set

$$(13) \qquad \theta_{\alpha\beta} = i_\alpha \theta p_\beta .$$

Clearly, $\theta_{\alpha\beta} \in \mathrm{Hom}(V_\alpha, V_\beta)$ as

$$V_\alpha \xrightarrow{i_\alpha} V \xrightarrow{\theta} V \xrightarrow{p_\beta} V_\beta \quad .$$

We call $\theta_{\alpha\beta}$ the matrix coefficients of θ. By a matrix, we mean for the moment simply a function f of two variables α, β which range over a set $\mathcal{J}$ of indices; the value $f(\alpha, \beta)$ is to belong to a given set $S_{\alpha\beta}$ which may depend on α and β. In our present case, $\mathcal{J} = \{1, 2, \ldots, q\}$ and $S_{\alpha\beta} = \mathrm{Hom}(V_\alpha, V_\beta)$. Thus, (13) defines a matrix which will be donoted by $[\theta]$ or by $[\theta_{\alpha\beta}]$. The letter α will always be reserved for the first of our two variables and β for the second variable. We often call α the row-index and β the column-index. If we wish to, we may write $[\theta]$ in the usual fashion

$$[\theta] = [\theta_{\alpha\beta}] = \begin{bmatrix} \theta_{11} & \theta_{12} & \cdots & \theta_{1q} \\ \theta_{21} & \theta_{22} & \cdots & \theta_{2q} \\ \cdot & \cdot & \cdot & \cdot \\ \theta_{q1} & \theta_{q2} & \cdots & \theta_{qq} \end{bmatrix} \quad ,$$

but this is only a question of notation.

Usually, when we speak of matrices, the sets $S_{\alpha\beta}$ satisfy the following further conditions: 1) $S_{\alpha\beta}$ is an additive abelian group. 2) The products of the elements $x \in S_{\alpha\gamma}$ with the elements $y \in S_{\gamma\beta}$ are defined as elements $xy \in S_{\alpha\beta}$ (for $\alpha, \beta, \gamma \in \mathcal{J}$). If the $[\theta_{\alpha\beta}]$ and $[\eta_{\alpha\beta}]$ are two matrices (with the same $\mathcal{J}$ and the same $S_{\alpha\beta}$), we can define the sum, and if $\mathcal{J}$ is finite, the product of the matrices in the usual manner

$$[\theta_{\alpha\beta}] + [\eta_{\alpha\beta}] = [\theta_{\alpha\beta} + \eta_{\alpha\beta}] ;$$

$$[\theta_{\alpha\beta}][\eta_{\alpha\beta}] = [\zeta_{\alpha\beta}] \text{ with } \zeta_{\alpha\beta} = \sum_{\gamma\in\mathcal{J}} \theta_{\alpha\gamma}\eta_{\gamma\beta} .$$

Usually, the addition and multiplication of elements of the various $S_{\alpha\beta}$ satisfy the following further rules

$$x(yz) = (xy)z \qquad \text{for } x \in S_{\alpha\gamma},\ y \in S_{\gamma\delta},\ z \in S_{\delta\beta}$$

$$x(y+z) = xy + xz \qquad \text{for } x \in S_{\alpha\gamma};\ y, z \in S_{\gamma\beta} ;$$

$$(y+z)x = yx + zx \qquad \text{for } y, z \in S_{\alpha\gamma};\ x \in S_{\gamma\beta} .$$

Then the matrices (with fixed finite $\mathcal{J}$) form a ring $\mathcal{M}$.

We can now state our Lemma:

(G) Let $V = \oplus\sum_{j=1}^{q} V_j$ be a Cartesian sum of q abelian groups V_j, all with the same set R of operators. Then the ring $\mathcal{E}(V)$ of R-endomorphisms of V is isomorphic with the ring $\mathcal{M}$ of matrices $[\theta_{\alpha\beta}]$ with

$$\mathcal{J} = \{1, 2, \ldots, q\};\ \alpha, \beta \in \mathcal{J};\ \theta_{\alpha\beta} \in S_{\alpha\beta} = \mathrm{Hom}(V_\alpha, V_\beta) .$$

Proof: Note first that for our sets $S_{\alpha\beta}$ and the usual definition of addition and multiplication of homomorphisms, the above conditions are satisfied.

If $\theta \in \mathcal{E}(V)$ has the matrix coefficients $\theta_{\alpha\beta} = i_\alpha \theta p_\beta$, we define a mapping ω of $\mathcal{E}(V)$ into $\mathcal{M}$ by mapping $\theta \longrightarrow [\theta] = [\theta_{\alpha\beta}]$. Clearly, this is an additive homomorphism. Further, if $\theta, \eta \in \mathcal{E}(V)$, then, by (12),

$$(\theta\eta)_{\alpha\beta} = i_\alpha\theta\eta p_\beta = i_\alpha\theta I\eta p_\beta = i_\alpha\theta\sum_{\gamma=1}^{q} p_\gamma i_\gamma\eta p_\beta$$

$$= \sum_{\gamma=1}^{q} i_\alpha\theta p_\gamma i_\gamma\eta p_\beta = \sum_{\gamma=1}^{q} \theta_{\alpha\gamma}\eta_{\gamma\beta} .$$

This proves that ω is a ring homomorphism.

Moreover, if elements $\theta_{\alpha\beta} \in \mathrm{Hom}\,(V_\alpha, V_\beta)$ are given arbitrarily for all $\alpha, \beta \in \mathcal{J}$ and if we set

$$\theta = \sum_{\rho,\sigma=1}^{q} p_\rho\theta_{\rho\sigma}i_\sigma ,$$

then $\theta \in \mathrm{Hom}(V, V)$, that is, $\theta \in \mathcal{E}(V)$. Further, by (12) $i_\alpha\theta p_\beta = \theta_{\alpha\beta}$. Thus θ has the prescribed matrix coefficients and ω maps $\mathcal{E}(V)$ onto $\mathfrak{M}$.

Finally, if $\theta \in \mathcal{E}(V)$ has the prescribed matrix coefficients $i_\alpha\theta p_\beta = \square$, then (12) shows that

$$\theta = I\,\theta I = \sum_{\alpha} p_\alpha i_\alpha\theta\sum_{\beta} p_\beta i_\beta = \square_{\alpha\beta} .$$

Hence, $\theta = \square$, that is, ω is an isomorphism and we are finished.

5. Structure of simple rings.

The results of section 2 and section 3 show that the study of semisimple m-rings can be reduced to that of simple m-rings R. We apply here the results of Chapter IV. Since a simple m-ring R has height $k = 1$ by (C), it follows from Definition 3 of Chapter IV that all indecomposable components of R are R-isomorphic. We may thus set

$$(14) \qquad R^{\cdot} = {}^{\bullet}\sum_{j=1}^{q} U_j \quad ,$$

where all U_j are R-isomorphic to the same indecomposable component X of R. Moreover, by Chapter IV, (L̲), the module X has the greatest proper submodule $Y = X \cap \mathrm{Rad}\,(R)$. Since $\mathrm{Rad}(R) = (0)$, this means that $Y = (0)$, that is, X is a simple module.

The direct sum ${}^{\bullet}\sum_{j=1}^{q} U_j$ in (14) is R-isomorphic to the Cartesian sum $\oplus\sum_{j=1}^{q} U_j$. Here, replace each term U_j by the R-isomorphic module X, that is, form

$$(15) \qquad V = \oplus \sum_{j=1}^{q} V_j \;, \text{ with } V_1 = V_2 = \dots = V_q = X.$$

Then $R^{\cdot} = {}^{\bullet}\sum_j U_j$ is R-isomorphic with V. This implies that $\mathcal{E}(R^{\cdot})$ and $\mathcal{E}(V)$ are ring-isomorphic.[*] Now, $\mathcal{E}(R^{\cdot})$ is a ring R' anti-isomorphic with R (Chapter IV, $\underline{F}_3$). On the other hand, Lemma (G̲) applied to (15) shows that $\mathcal{E}(V)$ is isomorphic to the ring $\mathfrak{M}$ of all q-rowed matrices $[\theta_{\alpha\beta}]$ with $\theta_{\alpha\beta} \in \mathrm{Hom}\,(V_\alpha, V_\beta) = \mathrm{Hom}\,(X, X)$, that is, with $\theta_{\alpha\beta} \in \mathcal{E}(X)$. Since X is a simple module, $\mathcal{E}(X)$ is a skew field T (Chapter IV, B̲)). Thus, $\mathfrak{M}$ is the ring of all q-rowed matrices with coefficients in the skew field T. We shall denote this ring $\mathfrak{M}$ by T_q. Thus, we have the ring-isomorphism

---

[*] Indeed, if Φ is an R-isomorphism of $R^{\cdot}$ onto V, then

$$\mathcal{E}(R^{\cdot}) = \Phi\, \mathcal{E}(V)\, \Phi^{-1} \approx \mathcal{E}(V)\,.$$

$$R' \approx T_q \; . \tag{16}$$

We wish to show that the simple ring R itself is a complete matrix ring over a skew field. If R satisfies the m-condition for ℓ-ideals (instead of that for r-ideals) then R' satisfies the m-condition for r-ideals. We may apply (16) to R' instead of R and since $(R')' \approx R$, we see that R is a complete matrix ring over a skew field.

If we wish to stick with rings with the m-condition for r-ideals, we note that if T and T' are anti-isomorphic rings, the rings T_q and T'_q are anti-isomorphic. Indeed, if $t \longrightarrow t'$ is a fixed anti-isomorphism of T onto T', a simple checking shows that

$$[t_{\alpha\beta}] \longrightarrow [t'_{\beta\alpha}] \qquad \begin{cases} t_{\alpha\beta} \in T \, ; \; \alpha, \beta = 1, 2, \dots, q; \\ \alpha \text{ row index}, \quad \beta \text{ column index} \end{cases}$$

is an anti-isomorphism of T_q onto T'_q. Take now the anti-isomorphic rings on both sides of (16) and set $D = T'$. Clearly, D is a skew field and we have

(H) Second Wedderburn Theorem. A simple m-ring R is isomorphic to a complete matrix ring D_q over a skew field D. Here, q is a fixed degree.

A slightly different transition from (16) to (H) will be given in Section 6.

6. The converse theorem and the uniqueness theorem.

(I) Let D be a skew field and let q be a natural integer. Then $R = D$ is a simple m-ring.

Proof: Let e_{ij} denote the q-rowed matrix which has the coefficient $1 \in D$ in its i-th row and j-th column while all other coefficients vanish (i,j fixed, $1 \leqq i, j \leqq q$). Then

$$(17) \qquad e_{ij}e_{rs} = \begin{cases} e_{is} & \text{for } j = r \\ 0 & \text{for } j \neq r \end{cases} .$$

Clearly

$$(18a) \qquad 1 = e_{11} + e_{22} + \ldots + e_{qq} = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 1 \end{bmatrix}$$

is the unit element of D_q. It follows from (17) that we have a resolution of $\mathbf{1}$ into q orthogonal idempotents. This corresponds to a decomposition

$$(18b) \qquad D_q = U_1 \dot{+} U_2 \dot{+} \ldots \dot{+} U_q \; ; \; U_h = e_{hh}D_q \, ,$$

cf. Chapter IV, (D).

The mapping $d \longrightarrow d\mathbf{1}$ with $d \in D$ is an isomorphism of D onto a subring of D_q. We identify d and $d\mathbf{1}$. Note that $d \in D$ then commutes with every e_{ij}. Moreover, the general element $[d_{ij}]$ of D_q can be written in the form

$$[d_{ij}] = \sum_{i,j=1}^{q} d_{ij}e_{ij} \; ; \quad (d_{ij} \in D) .$$

It follows from (17) that $U_h = e_{hh}D_q$ consists of the elements

$$u = \sum_{j=1}^{q} d_{hj}e_{hj}$$

with arbitrary $d_{hj} \in D_q$. These are the matrices in which all rows but the h-th row vanish while the coefficients in the h-th row are arbitrary. If $u \neq 0$, some $d_{hj} \neq 0$. Then $ud_{hj}^{-1}e_{jh} = e_{hh}$. Hence $e_{hh} \in uD_q$ and this implies $U_h = e_{hh}D_q \subseteq uD_q \subseteq U_h$, that is, $U_h = uD_q$. Since this holds for every $u \neq 0$ in U_h, the module U_h is simple. A simple group theoretical lemma (cf. Appendix, Section 5) shows that the m-condition holds for the module D_q in (18a), i.e., D_q is an m-ring. As a matter of fact the same proof shows that the maximum condition holds for the r-ideals of D_q. Then (18b) is a decomposition of D_q into indecomposable components. If U_h and U_r are two of these components, then $e_{hh} = e_{hr}e_{rh} \in U_hU_r$. Since e_{hh} is an idempotent, Chapter IV, ($\underline{X}$) shows that U_h and U_r are D_q-isomorphic. Hence D_q has the height 1 (p. 83).

Let $\nu \in \mathrm{Rad}(D_q)$. Since the representation $\mathfrak{U}_h$ with the simple module U_h is irreducible, we have $\mathfrak{U}_h(\nu) = \square$, that is $U_h \cdot \nu = (0)$. In particular, $e_{hh}\nu = 0$. Since this holds for all h, it follows from (18a) that $\nu = \mathbf{1}\nu = 0$. Hence $\mathrm{Rad}(D_q) = (0)$. Consequently, D_q is a semisimple m-ring of height 1. Now ($\underline{C}$) shows that D_q is simple, q.e.d.

The same arguments can be used for the proof of the uniqueness theorem:

(J) If $R \approx D_q$ where D is a given skew field, then q is uniquely determined by R and D is determined up to ring isomorphism.

Proof: We use the same notation as before. The D_q-module D_q has the composition series

$$U_1 \dot{+} U_2 \dot{+} \dots \dot{+} U_q \supset U_2 \dot{+} \dots \dot{+} U_{q-1} \supset \dots \supset U_{q-1} \dot{+} U_q \supset U_q \supset (0)$$

of length q. Since $R \approx D_q$, the R-module $R^{\cdot}$ has then also a composition series of length q. By the Jordan-Hoelder Theorem (Appendix, Section 4), the length of a composition series is uniquely determined. Hence q is uniquely determined by R.

Let $\mathfrak{F}$ be the irreducible representation of D_q with the module $U_1 = e_{11}D_q$. By Chapter IV, (F_2), the commuting ring $\mathcal{C}(\mathfrak{F})$ is anti-isomorphic with $e_{11}D_q e_{11}$. Clearly, $e_{11}D_q e_{11}$ consists of the martices

$$\begin{bmatrix} d & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{bmatrix} \qquad \text{with } d \in D$$

which form a ring isomorphic with D. Hence $\mathcal{C}(\mathfrak{F})$ is anti-isomorphic with D.

Let θ be an isomorphism of R onto D_q. Then

$$\theta\mathfrak{F} : \rho \xrightarrow{\theta} \rho^{\theta} \xrightarrow{\mathfrak{F}} \mathfrak{F}(\rho^{\theta}), \qquad (\rho \in R)$$

is an irreducible representation $\mathfrak{F}_0$ of R. Clearly, $\mathfrak{F}_0$ and $\mathfrak{F}$ have the same commuting ring $\mathcal{C}(\mathfrak{F}_0) = \mathcal{C}(\mathfrak{F})$. Since R is simple and hence of height 1, every irreducible representation of R

is anti-isomorphic to D and this shows that D is determined by R , apart from isomorphism.

We conclude this section with a number of remarks. First, we describe an alternate manner in which (H) can be obtained from (16). We have seen that (16) holds for all m-rings R. Now the proof of (I) shows that D_q is an m-ring, if D is a skew field. This shows that $R' \approx D_q$ is an m-ring too. Hence (16) can be applied to R' instead of R and it follows that (R')' is isomorphic with a complete matrix ring over a skew field and as $(R')' \approx R$, this yields (H) .

Next, we note

(K) If R is a semi-simple m-ring, not only the minimum condition but also the maximum condition holds for r-ideals. Moreover, both the minimum and the maximum condition holds for ℓ-ideals.

Proof: Because of (D) and the group theoretical lemma (Appendix Section 7) already used, it sufficies to prove (K) for simple m-rings R . Then, we may take $R = D_q$ where D is a skew field. As already remarked in the proof of (I), the maximum condition holds for the r-ideals of R. Furthermore, by (16) , $R' \approx T_q$ where T is a skew field. Hence the minimum and maximum condition hold for the r-ideals of R' and this means that both these conditions hold for the ℓ-ideals of R.

7. Structure of R-modules.

(L) Let R be a semisimple m-ring and let V be a unitary R-module (i.e., $v\mathbf{1} = v$ for $v \in V$). Then V is completely reducible, that is, V is a direct sum of simple modules.*

Proof: Let L be the sum of all simple submodules of V. As shown in the Appendix, Section 6, this "socle" L of V is completely reducible. We show that $L = V$. Suppose that this is not so and that there exist elements $v \in V$ with $v \notin L$. As in Chapter IV, (K), write R as a direct sum $R = \dot{\sum}_{i=1}^{n} U_i$ of indecomposable r-ideals U_i. By Chapter IV, (L), each U_i has the greatest proper submodule $W_i = U_i \cap \text{Rad}(R)$. Since $\text{Rad}(R) = (0)$, we have $W_i = (0)$, that is, U_i is simple. Since $v = v\mathbf{1} \in \sum_i vU_i$ and $v \notin L$, there exist indices i with $vU_i \nsubseteq L$. Now the mapping $u \longrightarrow vu$ with u running over U_i is a R-homomorphism of U_i onto vU_i. Since U_i is simple, the image vU_i is either simple or (0). Then, vU_i would belong to the sum L of all simple submodules of V, a contradiction.

The following two rules follow at once from general results on completely reducible groups (Appendix, Section 6).

(M) If R is a semisimple m-ring, if V is a unitary R-module and X a submodule of V, then V is the direct sum $V = X \dot{+} Y$ of X and another submodule Y of V.

---

*This can also be obtained from Chapter IV, Problem 19.

(N) If R is a semisimple m-ring and V a unitary R-module, the maximum condition and the minimum condition for submodules of V imply each other.

It is rather surprising that (N) remains valid for m-rings R which are not semisimple, provided that R has a unit element.

(O) Let R be an m-ring with unit element and let V be a unitary R-module. The minimum and maximum condition for submodules of V imply each other.

Proof: Let $N = \text{Rad}(R)$ and set $N^{o} = R$. Since N is nilpotent, $N^{h} = (0)$ for some natural integer h. By VN^{j}, we mean of course the submodule of V consisting of finite sums of terms $v\mu$ with $v \in V$, $\mu \in N^{j}$. Then

$$V = VN^{o} \supseteq VN^{1} \supseteq VN^{2} \supseteq \dots \supseteq VN^{h-1} \supseteq VN^{h} = (0).$$

It will be sufficient to prove that if either the minimum or the maximum condition for submodules of V is assumed, then V has a composition series (see the Appendix, Section 4). This will be shown, if we can find a composition series from VN^{j} to VN^{j+1}. Again, this is equivalent with finding a composition series of $X = VN^{j} / VN^{j+1}$.

Let $\lfloor t \rfloor$ denote the residue class (mod VN^{j+1}) of an element $t \in VN^{j}$. If $\nu \in N$, then $t\nu \in VN^{j+1}$ and hence $\lfloor t \rfloor \nu = \lfloor t\nu \rfloor = \lfloor 0 \rfloor$. Set $R^{*} = R/N$. We define now an R^{*}-module X^{*} consisting of the same elements $\lfloor t \rfloor$ as X and with the same addition. If $\rho^{*} \in R^{*}$ and if ρ is a corresponding element of R, set

$$\underline{|t|}\rho^* = \underline{|t|}\rho .$$

We may replace here ρ by $\rho + \nu$ with $\nu \in N$, but as $\underline{|t|}\nu = 0$, this does not change our product. Hence the product $\underline{|t|}\rho^*$ is well defined and it is now clear that a subset of X^* is a submodule, iff it forms a submodule of X.

By assumption, either the maximum or the minimum condition holds for submodules of V. It then follows that the corresponding condition holds for the submodules of $X = VN^j / VN^{j+1}$ and hence for the submodules of X^*. Since $R^* = R/N$ is a semisimple m-ring, (N) shows that both maximum and minimum conditions hold for submodules of X^* and then both these conditions hold for submodules of X. It follows that the module X has a composition series and this is what we had to prove.

(P) Corollary (Hopkins). If R is an m-ring with unit element, the maximum condition holds for r-ideals.

We only have to apply (O) to the module $V = R^\circ$. For m-rings without 1, (P) does not hold, see Problem 23 d.

Historical Note: As already remarked, the results of this chapter were obtained by Wedderburn for finite dimensional algebras. They were generalized by Artin for rings which satisfy both the maximum condition and the minimum condition. These conditions had first been introduced by Emmy Noether. Actually, the maximum condition was used only to show that the radical is nilpotent. It was noticed by Hopkins that one can dispense with this condition altogether for our theory. This fact is not particularly important in itself, but it is rather curious.

PROBLEMS TO CHAPTER V

I. Problems Related to Wedderburn's Theorems.

1. Suppose that a ring R is a sum $R = \sum S_i$ of subrings S_i and that $S_iS_j = (0)$ for $i \neq j$. Show that each S_i is an ideal of R. If each S_i has a unit element, show that the sum $\sum_i S_i$ is direct.

2. Show that the center of a Cartesian sum of rings R_i is the Cartesian sum of the centers of the R_i. Show that if R is a complete matrix ring S_q over a ring S with unit element, the center of R consists of the elements cI where c is in the center of S and I is the unit matrix. Use these results to show that the center of a semi-simple m-ring of height k is isomorphic with a Cartesian sum of k fields.

3. Let R be a ring with 1 . A prime ideal P of R is an ideal $P \neq R$ of R such that if a projuct AB of two ideals lies in P, at least one factor lies in P.

(a) Show that this condition can be replaced by the following one: If a product AB of two ideals $A \supseteq P$, $B \supseteq P$ lies in P, at least one factor is P.

(b) Show that a maximal ideal of a ring R is a prime ideal, but that the converse need not be true.

(c) Show that if R is an m-ring with 1 , every prime ideal is maximal. If R has height k, show that R has exactly k distinct prime ideals and these are the kernels of the k "distinct" irreducible representations of R.

(d) If R is commutative, show that an ideal $P \neq R$ is a prime ideal, iff the conditions $ab \equiv 0 \pmod{P}$ with $a, b \in R$ imply $a \equiv 0 \pmod{P}$ or $b \equiv 0$ (Mod P).

4. (a) Let R be an m-ring with 1. Show that if V is a free module with a finite number n of free generators, then n is uniquely determined by V. We may then define n as dimension $\dim_R V$.

(b) Show that this result need not hold, if R is not an m-ring.

Hints: (a) Use Jordan-Hoelder. (b) Apply Chapter I, Problem 6.

5. Give an alternate proof of Wedderburn's first theorem using Problem 17 of Chapter IV.

Hint: Show that a semisimple m-ring is a direct sum of ideals each of which is a sum of isomorphic simple modules.

6. Modify the proof of (H) in such a way that both Wedderburn's theorems are obtained simultaneously.

Suggested procedure: Let R be a semisimple m-ring and write $R = \cdot\sum_{i=1}^{k} \cdot\sum_{\lambda=1}^{q_i} U_i^{(\lambda)}$ where the $U_i^{(\lambda)}$ are indecomposable components and where $U_i^{(\lambda)} \approx U_j^{(\mu)}$, iff $i = j$. Form the module $V = \oplus\sum_{i=1}^{k} (\oplus\sum_{\lambda=1}^{q_i} V_i^{(\lambda)})$ with $V_i^{(\lambda)} = U_i^{(1)}$ for $1 \leqq \lambda \leqq q_i$. Use the method in the proof of (H) to show that R is isomorphic with a Cartesian sum of rings which are complete matrix rings over skew fields.

7. Let R be a simple ring with a unit element and assume that R has minimal r-ideals $A \supset (0)$ but do not assume the m-condition. Give as elementary a proof as possible for Wedderburn's second theorem using the following procedure:

1) Show that A contains idempotents e and that $A = eA = eR$.

2) Show that $D = eRe$ is a skew field and that $V = eR$ is a left vector space over D.

3) Show that if θ is a D-linear transformation of $V \longrightarrow V$ and if $\sum_{i=1}^{n} r_i v_i = 0$ with $r_i \in R$, $v_i \in V$, then $\sum_{i=1}^{n} r_i(v_i\theta) = 0$. Show further that then θ can be extended to an operator-homomorphism θ^* of ${}^\cdot R$ (i.e., of R considered as an R-left module).

4) Show that every θ in 3) is a right multiplication $R(c)$ of R with $c \in R$. Prove that R is isomorphic with the ring of all D-linear transformation of $V \longrightarrow V$ and that V is finite dimensional as a D-space.

8. Let R be a semisimple m-ring with unit element how that every unitary R-module is both projective and injective.

Hint: Use (L) and, for the injectivity, Problem 5 of Chapter IV.

9. Let R be a ring with unit element. Show that each of the following conditions is necessary and sufficient in order that R be a semisimple m-ring:

(α) $R^\cdot$ is a direct sum of simple modules.

(β) Each simple unitary R-module is projective.

(γ) Each maximal r-ideal is an injective module.

(δ) Each r-ideal $\neq (0)$ is a component of R.

Hints: After proving (α), we can prove that R is a semisimple m-ring by showing that $R^\bullet$ has the socle $R^\bullet$. Use # 8 and the connection between simple modules and maximal r-ideals (Chapter II).

II. Primary and Uniserial Rings.

10. Let R be an m-ring with a unit element. Show that the following three conditions are equivalent:

(a) $R/\mathrm{Rad}(R)$ is simple.

(b) Every ideal $\neq R$ of R is nilpotent.

(c) The height of R is 1.

If these conditions are satisfied, R is said to be primary.

11. Let R be an m-ring with a unit element. Show that the following three conditions are equivalent:

(a) $R/\mathrm{Rad}(R)$ is a skew field.

(b) Every r-ideal $\neq R$ of R is nilpotent.

(c) The R_r-module $R^\bullet$ is indecomposable.

If these conditions are satisfied, R is said to be completely primary.

12. Show that a primary m-ring R is isomorphic with a complete matrix ring S over a completely primary m-ring S.

Hint: In a full decomposition of R, all components are isomorphic (# 10). Use a method similar to that in the proof of (H). If e is an idempotent in the corresponding resolution of 1, we may take $S = eRe$.

13. Let R be an m-ring. Use # 10 for an alternate proof that a ring R is simple, iff it is semisimple of height 1.

EFINITION An m-ring with 1 is quasi-uniserial if for every indecomposable component U of R, the module $W = U \cap \mathrm{Rad}(R)$ is either (0) or has itself a greatest proper submodule Z. If, in addition, in the latter case U/W and W/Z are R-isomorphic, we call R a uniserial ring. [In the literature, these rings are usually called "generalized uniserial rings" and the tern "uniserial" is reserved for what we call primary uniserial rings or uniserial ring of height 1.]

14. Let R be a quasi-uniserial ring of height k.

(a) Show that every indecomposable component U_i of R has a unique composition series $U = W_i^{(0)} \supset W_i^{(1)} \supset W_i^{(2)} \supset \ldots$.

(b) Let $U_1, U_2, \ldots, U_k$ be a full system of non-isomorphic indecomposable components of R and set $U_i/W_i^{(1)} = F_i$. Show that to every index j with $1 \leqq j \leqq k$, there belongs an index j* such that if $W_i^{(r-1)}/W_i^{(r)} \approx F_j$ for some i and r and if $W_i^{(r)} \neq (0)$, then $W_i^{(r)}/W_i^{(r+1)} \approx F_{j*}$.

(c) Show that every submodule of U_i is isomorphic with a quotient module of some U_j.

Hint: Use induction. Apply Chapter IV, Problem 12.

15. (Continuation). Let R be uniserial.

(a) Show that $W_i^{(\lambda-1)}/W_i^{(\lambda)} \approx U_i/W_i$ for all λ.

(b) Show that each submodule of U_i is R-isomorphic with a quotient module of U_i.

(c) Show that a uniserial ring of height k is isomorphic with a Cartesian sum of k primary uniserial rings.

(d) Obtain Wedderburn's first theorem as a special case.

Hint: In (c), use Problem 17 of Chapter IV.

16. Let R be an m-ring with 1 and set $N = \mathrm{Rad}(R)$.

(a) Show that R is quasi-uniserial, iff for every indecomposable idempotent e of R with $eN \neq (0)$, eN/eN^2 is simple. Show further that if this is so, the unique composition series of eR is $eR \supset eN \supset eN^2 \supset eN^3 \supset \dots$.

(b) Show that a quasi-uniserial ring R is uniserial, if for every indecomposable idempotent e with $eN \neq (0)$, there exists an element $f \in eNe$ with $f \notin N^2$.

Hint: Apply Chapter IV, Problem 20. Note that if R is an m-ring with 1 and if e is an idempotent, the upper Loewy series of eR is $eR \supset eN \supset eN^2 \supset$

III. Commutative Rings.

DEFINITIONS. An integral domain is a commutative ring R with unit element such that the product of two elements of R vanishes only, if a factor is 0. Then R can be imbedded in a quotient field (e.g., by Problem 13 of Chapter We do not count the ideal (0) among the prime ideals. An element z of an extension field Ω of R is integral with regard to R, if z belongs to a subring T of Ω which is a finitely generated R-module. This is equivalent with saying that z satisfies an equation $z^n + c_1 z^{n-1} + \dots + c_n = 0$ with $c_j \in R$. (Why?) The ring R is integrally closed in Ω, if all $z \in \Omega$ which are integral with regard to R lie in R.

We say that the restricted m-condition (m*) holds in R, if for every ideal $A \neq (0)$, the ring R/A is an m-ring. This is the same as to say that the m-condition holds for all families of ideals of R such that some ideal $A \neq (0)$ is included in all ideals of the family.

17. Let R be a commutative m-ring with 1.

(a) Show that R is a direct sum $R = \dot{\sum}_{i=1}^{k} U_i$ of k indecomposable modules no two of which are R-isomorphic. Note that $U_i U_j = (0)$ for $i \neq j$.

(b) Show that the irreducible representation $\mathfrak{U}_i$ in U_i has only one irreducible constituent $\mathfrak{F}_i$ (with a certain multiplicity $\geqq 1$).

(c) Show that if R is quasi-uniserial, it is uniserial.

(d) Show that if R is primary, it is completely primary.

Hint: For (b), apply Problem 16 of Chapter IV.

18. Let R be an integral domain which satisfies the restricted minimum condition (m*).

(a) Show that every ideal of R is a finitely generated R-module.

(b) Show that an ideal $P \neq (0)$, R is a prime ideal of R, iff P is maximal, i.e., iff R/P is a field. Show further that if A is an ideal $\neq (0)$, R, there exists only a finite number of distinct prime ideals $P_1, P_2, \ldots, P_n \supseteq A$ and, for a suitable exponent h, $(P_1 P_2 \ldots P_n)^h \subseteq A$.

(c) Set $Q_i = P_i^h + A$ in (b). Show that $A = Q_1 Q_2 \ldots Q_n$ and that P_i is the only prime ideal $\supseteq Q_i$.

Hints: (a) Note that the maximum condition holds for ideals. (b) Apply #3.

19. Let R be an integral domain which satisfies the restricted m-condition (m*). Let P be a prime ideal.

(a) Show that $P, P^2, P^3, \dots$ are all distinct and that $\bigcap_{n=0}^{\infty} P^n = (0)$.

(b) We say that P is normal, if P/P^2 is a simple R-module. Show that then every ideal $H \supseteq P^n$ has the form P^j with $0 \leqq j \leqq n$.

Hints: (a) If $P^n = P^{n+1}$, set $P^n = \sum_{j=1}^{r} \alpha_j R$ with $\alpha_j \in R$, (# 18a). Obtain equations $\alpha_i = \sum_{j=1}^{r} p_{ij}\alpha_j$ with $p_{ij} \in P$, $j = 1, 2, \dots, n$ and get a contradiction from $\det([p_{ij}] - I) = 0$. (b) Show that $R_o = R/P^n$ is uniserial.

20. A Dedekind domain R can be defined as an integral domain such that

(I) the restricted m-condition (m*) holds.

(II) every prime ideal P is normal (cf. # 19.)

Show that in a Dedekind domain, every ideal $\neq (0)$, R can be written as a product of prime ideals in a unique manner. Moreover, if $P_1, P_2, \dots, P$ are distinct prime ideals, show that $P_1^{r_1} P_2^{r_2} \dots P_n^{r_n} \supseteq P_1^{s_1} P_2^{s_2} \dots P_n^{s}$ (with $r_i \geqq 0$, $s_i \geqq 0$), iff $r_1 \leqq s_1$, $r_2 \leqq s_2$, $\dots$, $r_n \leqq s_n$.

Hint: Apply # 18, # 19.

21. Let R be an integral domain with the quotient field F. Let P be a maximal ideal of R and let Q be the additive subgroup of F defined by $Q = \{x \mid xP \subseteq R, x \in F\}$.

(a) Show that either $PQ = R$ or $PQ = P$.

(b) Show that if $PQ = R$, then P/P^2 is a simple R-module $\neq 0$.

(c) Using #18 show that if the condition (m*) holds for R then $Q \supset R$.

22. Use the preceding problems to show: An integral domain R is a Dedekind domain, iff the following two conditions hold:

(I) The restricted m-condition (m*) holds in R. (II) R is integrally closed in its quotient field.

IV. Some examples

23. Give examples to illustrate the following points:

(a) The radical of an m-ring need not be an m-ring.

(b) Not every nilpotent ring R appears as the radical of an m-ring.

(c) There exist rings such that the m-condition holds for right ideals but not for left ideals.

(d) There exist m-rings (without unit element) which do not satisfy the maximum condition for right ideals.

CHAPTER VI

THE GENERAL STRUCTURE THEOREM FOR m-RINGS

The methods of Chapter V can be used to prove a structure theorem for m-rings which contains Wedderburn's theorems as special cases. In order to describe the results, we need a definition.

Definition 1. A ring S is a reduced ring, if $S/\operatorname{Rad}(S)$ is isomorphic with a Cartesian direct sum of a finite number k of skew fields. The number k will be called the height of S. We include the case $k = 0$, $S = (0)$.

We shall see that the definition of height coincides with that given in Chapter IV (in the case of m-rings).

If R is an arbitrary m-ring of height k, we shall associate with R a reduced m-ring S of height k and a system of k "degrees" $q_1, q_2, \dots, q_k$. It will be shown that R is determined by S and the system $\{q_i\}$ (apart from isomorphism). Again, we shall prove a converse theorem and a uniqueness theorem.

This shows that the problem of constructing all m-rings can be replaced by that of constructing all reduced m-rings.

The results of Chapter VI will be used only occasionally later on and a reader who omits the chapter will not miss too much.

1. Statement of the general structure theorem.

The theorem takes a somewhat simpler form for rings with unit element and we shall first state it for this case.

Definition 2: Let S be a reduced ring of height k with a unit element. Let $\{e\} = \{e_1, e_2, \dots, e_k\}$ be a system of k orthogonal idempotents of S and let $\{q\} = \{q_1, q_2, \dots, q_k\}$ be a system of k natural integers. Denote by C_1 the set of all ordered pairs $\tau = (i, \lambda)$ with $1 \leqq i \leqq k$, $1 \leqq \lambda \leqq q_i$ and set $e_\tau = e_i$ for $\tau = (i, \lambda) \in C_1$. The checkered matrix ring $M_1 = M_1(S, \{e\}, \{q\})$ is the ring of all matrices

$$(1) \qquad [m_{\tau\omega}] \; ; \; \tau, \omega \in C_1 \; ; \quad \left\{ \begin{array}{l} \tau \text{ row index} \\ \omega \text{ column index} \end{array} \right.$$

such that $m_{\tau\omega} \in e_\tau S e_\omega$.

It is quite obvious that the matrices (1) form a ring. If the elements of C_1 are arranged lexicographically and if matrices are written in the usual manner as square arrays of coefficients, each matrix of M is subdivided into rectangles in a checkerboard fashion such that in each rectangle the coefficients belong to a set $e_i S e_j$.

(A) If R is an m-ring with unit element, there exists a reduced m-ring S, also with unit element, such that R is isomorphic with a checkered matrix ring $M_1(S, \{e\}, \{q\})$.

In order to deal with the general case, we modify Definition 2:

Definition 2*: Let S be a reduced m-ring of height k and let $\{e\}$ and $\{q\}$ have the same significance as in Definition 2. Imbed S in an extended ring $S^{\#}$ with a unit element 1_0 (Chapter II, Section 9). Set

(2) $$e_0 = 1_0 - \sum_{i=1}^{k} e_i, \quad q_0 = 1 .$$

Let C denote the set of all ordered pairs (i, λ) with $0 \leqq i \leqq k$, $1 \leqq \lambda \leqq q_i$ and set $e_\tau = e_i$ for $\tau = (i, \lambda) \in C$. The checkered matrix ring $M = M(S, \{e\}, \{q\})$ is the ring of all matrices

(1*) $$[m_{\tau\omega}] ; \ \tau, \omega \in C ; \left\{ \begin{array}{l} \tau \ \text{row index} \\ \omega \ \text{column index} \end{array} \right.$$

such that

(1**) $$m_{\tau\omega} \in e_\tau S e_\omega \quad \text{(for all } \tau, \omega \in C \text{)}.$$

The only difference between the matrices (1) and (1*) is that in (1*) we added one row (belonging to $\tau = (0, 1)$) and one column (belonging to $\omega = (0, 1)$) . If S has a unit element, this row and column consist of coefficients zero as we shall see. For this reason, it will not be necessary to distinguish carefully between M and M_1 here.

(A*) Theorem 1 : If R is an m-ring, there exists a reduced m-ring S such that R is isomorphic with a checkered matrix ring $M(S, \{e\}, \{q\})$.

The proof of (A) is somewhat simpler than that of (A*) . It is not necessary to use the results of Chapter IV, Section 5 and there is no need to work with the extended rings. In order to avoid repetitions, we shall prove (A*) in Section 2 and deduce (A) from it. The simplifications possible in a direct proof of (A) are fairly obvious.

2. Proof of Theorem 1

Let R be a ring and let $R^{\#}$ denote the extended ring with a unit element $\mathbb{1}$. For convenient reference, we give two propositions stating simple facts concerning idempotents and homomorphisms.

(B) Let e and e^* be idempotents of $R^{\#}$. 1) We have $ex = x$ for $x \in eR^{\#}$, and $xe^* = x$ for $x \in R^{\#}e^*$. 2) If Y is a left ideal of $R^{\#}$, then $eR^{\#} \cap Y = eY$. 3) If H is an ideal of $R^{\#}$, then $eR^{\#}e^* \cap H = eHe^*$. 4) If $e \in R$, then $eR = eR^{\#}$. 5) If at least one of e, e^* belongs to R, then $eRe^* = eR^{\#}e^*$. 6) If $ee^* = 0$, at least one of e, e^* belongs to R.

Proof: 1) is obvious. In 2), it is clear that $eY \subseteq eR^{\#} \cap Y$. If $y \in eR^{\#} \cap Y$, then $y = ey \in eY$. Hence $eR^{\#} \cap Y \subseteq eY$ and we have equality. The proof of 3) is similar. If e belongs to the ideal R of $R^{\#}$, then $eR^{\#} \subseteq R$ and hence $eR^{\#} \subseteq eR$ which implies $eR^{\#} = eR$. The proof of 5) is similar. Finally, if $\mathbb{Z}$ is the ring of rational integers, we may set $e = r + n\mathbb{1}$, $e^* = r^* + n^*\mathbb{1}$ with $r, r^* \in R$ and $n, n^* \in \mathbb{Z}$. If $ee^* = 0$, then $nn^* = 0$. Hence $n = 0$ or $n^* = 0$, that is $e \in R$ or $e^* \in R$.

If θ is a mapping of a set A and if B is a subset, the restriction of θ to B will be denoted by $\theta \mid B$. If c is an element of $R^{\#}$, as before $\mathcal{L}(c)$ will denote the left multiplication by c in $R^{\#}$, i.e., the mapping $x \longrightarrow cx$ of $R^{\#}$ onto itself.

(C) Let e and e^* be two idempotents of $R^{\#}$ and set $U = eR^{\#}$, $U^* = e^*R^{\#}$.

1) The set $\mathrm{Hom}(U^*, U)$ of the $R^{\#}$-homomorphisms of U^* into U consists of the mappings $\mathcal{L}(c) \mid U^*$ with $c \in eR^{\#}e^*$.

2) The mapping $\mathcal{L}(c) \mid U^*$ with $c \in eR^{\#}e^*$ is an $R^{\#}$-isomorphism of U^* onto U, iff there exists an element $c^* \in e^*R^{\#}e$ with

$$(3) \qquad cc^* = e\,, \quad c^*c = e^* \quad .$$

3) If H is a left ideal of $R^{\#}$, an $R^{\#}$-isomorphism of U^* onto U maps $U^* \cap H$ onto $U \cap H$.

4) The ring $\mathcal{E}(U)$ of $R^{\#}$-endomorphisms of U consists of the elements $\mathcal{L}(c) \mid U$ with $c \in eR^{\#}e$. The mapping $c \longrightarrow \mathcal{L}(c) \mid U$ is an anti-isomorphism of $eR^{\#}e$ onto $\mathcal{E}(U)$.

Proof: 1) cf. Chapter IV, (F). If $\theta \in \mathrm{Hom}(U^*, U)$ maps $e^* \longrightarrow c$, then $e^*x \longrightarrow cx$ for $x \in R^{\#}$. If $x = e^*$, $e^*x = e^*$ and hence $ce^* = c$. Thus, $e^*x \longrightarrow ce^*x$, that is, $\theta = \mathcal{L}(c) \mid U^*$. Since $c \in eR^{\#}$, we have $c = ec$ and then $c = ece^* \in eR^{\#}e^*$. Conversely, for $c \in eR^{\#}e^*$, $\mathcal{L}(c) \mid U^* \in \mathrm{Hom}(U^*, U)$.

2) Set $\theta = \mathcal{L}(c) \mid U^*$ with $c \in eR^{\#}e^*$. Clearly, θ is an $R^{\#}$-isomorphism of U^* onto U, iff there exists a reciprocal mapping $\theta \in \mathrm{Hom}(U, U^*)$ such that $\theta\theta^*$ is the identity map $I \mid U^*$ of U^* and that $\theta^*\theta$ is the identity map $I \mid U$ of U. By 1), θ^* must have the form $\mathcal{L}(c^*) \mid U$ with $c^* \in e^*R^{\#}e$. Now, $e^*\theta\theta^* = ce^*\theta^* = c\theta^* = c^*c$ and $e\theta^*\theta = c^*\theta = cc^*$. Clearly, $\theta\theta^* = I \mid U^*$, iff $e^*\theta\theta^* = e^*$ and $\theta^*\theta = I \mid U$, iff $e\theta^*\theta = e$. Thus, θ will be an $R^{\#}$-isomorphism of U onto U^*, iff there exists $c^* \in e^*R^{\#}e$ satisfying (3).

3) If H is a left ideal, every left multiplication $\mathcal{L}(c)$ maps $H \longrightarrow cH \subseteq H$. If θ is an $R^{\#}$-isomorphism of U^* onto U, θ maps $U^* \cap H \longrightarrow U \cap H$. For the same reason, θ^{-1} maps $U \cap H \longrightarrow U^* \cap H$ and hence θ maps $U^* \cap H$ onto $U \cap H$.

4) cf. Chapter IV, ($\underline{F}_2$). The first part is the special case $e = e^*$ of 1) and the second part is obvious.

Assume now that R is an m-ring. We begin with the proof of Theorem 1. According to Chapter IV, ($\underline{S}$), ($\underline{S}^*$) there exist decompositions of $R^{\#}$ into indecomposable components. We write such a decomposition in the form

$$R^{\#} = \cdot \sum_{i=0}^{k} \cdot \sum_{\lambda=1}^{q_i} U_i^{(\lambda)} \tag{4}$$

where the notation is chosen such that $U_i^{(\lambda)}$ and $U_j^{(\mu)}$ are $R^{\#}$-isomorphic, iff $i = j$. Let

$$\mathbb{1} = \sum_{i=0}^{k} \sum_{\lambda=1}^{q_i} e_i^{(\lambda)} \tag{5}$$

be the corresponding resolution of $\mathbb{1}$ into orthogonal idempotents, $e_i^{(\lambda)} \in U_i^{(\lambda)}$. Since $\mathbb{1} \notin R$, we may choose our notation such that $e_0^{(1)} \notin R$. By ($\underline{B6}$), then all other $e_i^{(\lambda)}$ belong to R and this implies $U_i^{(\lambda)} = e_i^{(\lambda)} R^{\#} \subseteq R$, except for $i = 0$, $\lambda = 1$. It follows from ($\underline{C3}$) with $H = R$ that $U_0^{(1)} \not\subseteq R$ cannot be $R^{\#}$-isomorphic with some $U_i^{(\lambda)} \subseteq R$. Hence $q_0 = 1$. Moreover, we have (cf. ($\underline{B4}$)),

$$(6) \qquad U_i^{(\lambda)} = e_i^{(\lambda)}R^{\#} = e_i^{(\lambda)}R \subseteq R \qquad (\text{for } i > 0).$$

It will be convenient to set

$$U_\tau = U_i^{(1)} = U_i\,, \quad e_\tau = e_i^{(1)} = e_i$$

for $\tau = (i, \lambda) \in C\,;\ 0 \leqq i \leqq k\ ,\ 1 \leqq \lambda \leqq q_i$. (cf. Definition 2*).

Again, the notation $R^{\#\cdot}$ is to indicate that $R^{\#}$ is to be looked upon as an $R^{\#}$-module. Then $R^{\#\cdot}$ is $R^{\#}$-isomorphic with the module

$$(7) \qquad V = \oplus \sum_{\tau \in C} U_\tau\,.$$

Indeed, let $\overline{U}_\tau$ denote the submodule of V obtained from U_τ by injection. Since $U_i^{(\lambda)}$ is $R^{\#}$-isomorphic with U_τ for $\tau = (i, \lambda)$, we can find an $R^{\#}$-isomorphism φ of $R^{\#\cdot}$ onto V such that $U_i^{(\lambda)}$ in (4) is mapped isomorphically onto the corresponding U_τ in (7).

Since $R^{\#\cdot}$ and $V = R^{\#\cdot}\varphi$ are $R^{\#}$-isomorphic, their endomorphism rings $\mathcal{E}(R^{\#\cdot})$ and $\mathcal{E}(V) = \varphi^{-1}\{\mathcal{L}\}\varphi$ are ring isomorphic. Here, $\mathcal{E}(R^{\#\cdot})$ is the ring $\{\mathcal{L}\}$ consisting of the left multiplications $\mathcal{L}(c)$ with $c \in R^{\#}$ (for instance, by (C4)). Thus

$$(8) \qquad \{\mathcal{L}\} \approx \mathcal{E}(V) = \varphi^{-1}\{\mathcal{L}\}\varphi\,.$$

By Chapter V, (G) , the endomorphism ring $\mathcal{E}(V)$ of the Cartesiam sum (7) is isomorphic with the ring of all matrices

$$(9) \qquad [\theta_{\omega\tau}];\ \omega, \tau \in C;\ \begin{cases} \omega \text{ row index} \\ \tau \text{ column index} \end{cases}$$

such that each $\theta_{\omega\tau}$ is an arbitrary element of $\mathrm{Hom}(U_\omega, U_\tau)$. By ($\underline{\mathrm{C}1}$), we may then set $\theta_{\omega\tau} = \mathcal{L}(m_{\tau\omega})\,|U_\omega$ where each $m_{\tau\omega}$ is an arbitrary element of $e_\tau R^{\#} e_\omega$. Then, the matrix (9) takes the form $[\mathcal{L}(m_{\tau\omega})\mid U_\omega]$. It is seen at once that if we replace this matrix by $[\mathcal{L}(m_{\tau\omega})]$, we obtain an isomorphic ring $\mathcal{X}$. Combining this with (8), we have

$$(10) \qquad \{\mathcal{L}\} \approx \mathcal{X}.$$

The ring $R^{\#}$ is anti-isomorphic to $\{\mathcal{L}\}$. Thus if $\mathfrak{M}$ is a ring anti-isomorphic with $\mathcal{X}$, then $R^{\#} \approx \mathfrak{M}$. As in Chapter V, Section 5, such a ring $\mathfrak{M}$ is obtained by performing the following two operations on all matrices $[\mathcal{L}(m_{\tau\omega})] \in \mathcal{X}$:

1) Interchange the role of the row index ω and the column index τ.

2) Replace each coefficient $\mathcal{L}(m_{\tau\omega})$ by the corresponding element of an anti-isomorphic ring.

Since $c \longrightarrow \mathcal{L}(c)$ is an anti-isomorphism of $R^{\#}$ onto $\{\mathcal{L}\}$, 2) can be accomplished by replacing $\mathcal{L}(m_{\tau\omega})$ by $m_{\tau\omega}$ in our matrices. It follows now that $R^{\#}$ is isomorphic with the ring $\mathfrak{M}$ of all matrices

$$(11) \qquad [m_{\tau\omega}];\ \tau, \omega \in C;\ \begin{cases} \tau \text{ row index} \\ \omega \text{ column index} \end{cases}$$

such that $m_{\tau\omega} \in e_\tau R^{\#} e_\omega$ for all τ, ω.

Since we are mainly interested in the ring R and not in $R^{\#}$, we determine the subring of $\mathfrak{M}$ on which R is mapped by the isomorphism of $R^{\#}$ onto $\mathcal{M}$. More generally, we determine the image in $\mathcal{M}$ of an arbitrary ideal H of $R^{\#}$. We prove

(D) Lemma: The isomorphism of $R^{\#}$ onto the ring $\mathcal{M}$ of matrices (11) maps the ideal H onto the set of matrices (11) whose coefficients $m_{\tau\omega}$ all belong to H.

Proof: For the proof of (D) , it is necessary to reexamine the preceding considerations.

The anti-isomorphism $c \longrightarrow \mathcal{L}(c)$ maps H onto $\mathcal{L}(H) = \{\mathcal{L}(c) | c \in H\} \subseteq \{\mathcal{L}$ Then, (D) is equivalent with saying that the isomorphism (10) maps $\mathcal{L}(H)$ onto the set of matrices $[\mathcal{L}(m_{\tau\omega})] \in \mathfrak{X}$ for which $m_{\tau\omega} \in H$ for all τ and ω .

Let $c \in R^{\#}$. The left multiplication $\mathcal{L}(c)$ of $R^{\#}$ maps $R^{\#}$ onto $cR^{\#}$. If $c \in H$, then $cR^{\#} \subseteq H$. Conversely, if $cR^{\#} \subseteq H$, we have $c = c1 \in H$. Thus, $\mathcal{L}(H)$ consists of those $\mathcal{L}(c)$ with $c \in R^{\#}$ which map $R \longrightarrow H$. It follows from (5) that $H = \bullet\sum_i \bullet \sum_\lambda e_i^{(\lambda)}H$. By (B2), $e_i^{(\lambda)}H = U_i^{(\lambda)} \cap H$. Thus, $\mathcal{L}(c) \in \mathcal{L}(H)$, iff $\mathcal{L}(c)$ maps

$$R^{\#} = \bullet\sum_{i} \bullet \sum_{\lambda} U_i^{(\lambda)} \longrightarrow H = \bullet \sum_{i} \bullet \sum_{\lambda} (U_i^{(\lambda)} \cap H). \tag{12}$$

The isomorphism of $\{\mathcal{L}\}$ onto $\mathfrak{f}(V)$ in (8) maps $\mathcal{L}(c)$ on $\theta = \varphi^{-1}\mathcal{L}(c)\varphi$. It is obvious that $\mathcal{L}(c)$ satisfies the condition (12) , iff θ maps $V = (R^{\#\bullet})\varphi$ into $H\varphi$. Since φ mapped $U_i^{(\lambda)}$ onto U_τ with $\tau = (i, \lambda)$, (C3) shows that φ maps $U_i^{(\lambda)} \cap H$ onto $U_\tau \cap H$. Hence $H\varphi = \oplus \sum_\tau (U_\tau \cap H)$ and $\mathcal{L}(c)$ satisfies (12), iff $\theta = \varphi^{-1}\mathcal{L}(c)\varphi$ maps

(13) $$V = \oplus \sum_{\tau} U_{\tau} \longrightarrow \oplus \sum_{\tau} U_{\tau} \cap H .$$

Clearly, (13) holds, iff the "matrix coefficient" $\theta_{\omega\tau}$ of θ maps $U_{\omega} \longrightarrow U_{\tau} \cap H$ for all τ and ω. If we set $\theta_{\omega\tau} = \mathcal{L}(m_{\tau\omega})|U_{\omega}$ with $m_{\tau\omega} \in e_{\tau}R^{\#}e_{\omega}$, then : $U_{\omega}\theta_{\omega\tau} = m_{\tau\omega}U_{\omega}$. If $m_{\tau\omega} \in H$, then $m_{\tau\omega}U_{\omega} \subseteq H$ and hence $m_{\tau\omega}U_{\omega} \subseteq U_{\tau} \cap H$. Conversely, if $m_{\tau\omega}U_{\omega} \subseteq H$, then $m_{\tau\omega}e_{\omega} \in H$. Thus, the isomorphism (10) maps $\mathcal{L}(H)$ onto the set of matrices $[\mathcal{L}(m_{\tau\omega})] \in \mathcal{X}$ for which $m_{\tau\omega} \in H$ for all τ, and this concludes the proof of (**D**).

Since the coefficient $m_{\tau\omega}$ of (11) belongs to $e_{\tau}R^{\#}e_{\omega}$, it follows from (**B3**) that $m_{\tau\omega} \in H$, iff

(14) $$m_{\tau\omega} \in e_{\tau}R^{\#}e_{\omega} \cap H = e_{\tau}He_{\omega}.$$

Set

(15) $$1_0 = e_0 + e_1 + \dots + e_k .$$

As a sum of orthogonal idempotents, 1_0 is an idempotent. If we set

(16) $$S^{\#} = 1_0 R^{\#} 1_0 , \quad S = 1_0 R 1_0 ,$$

it is clear that $S^{\#}$ is a ring with a unit element 1_0 and that S is a subring. We shall see below that $S^{\#}$ is the extended ring belonging to S as indicated by the notation.

It follows from (15) that $e_i = 1_0 e_i = e_i 1_0$, for $i = 0,1, \dots, k$.

Hence $e_i = \mathbb{1}_0 e_i \mathbb{1}_0 \in \mathbb{1}_0 R^{\#} \mathbb{1}_0 = S^{\#}$. For $i > 0$, $e_i \in R$ by (6) and hence $e_i \in S$. Since $e_\tau = e_i$ for $\tau = (i, \lambda)$, all e_τ belong to $S^{\#}$.

Take now H as the ideal R of $R^{\#}$. Our result shows that R is isomorphic with the subset M of $\mathfrak{M}$ consisting of those matrices (11) whose coefficients satisfy the conditions $m_{\tau\omega} \in e_\tau R e_\omega$. Since $e_\tau = e_\tau \mathbb{1}_0$, $e_\omega = \mathbb{1}_0 e_\omega$, these conditions can be written in the form $m_{\tau\omega} \in e_\tau \mathbb{1}_0 R \mathbb{1}_0 e_\omega = e_\tau S e_\omega$. These are exactly the conditions (1**). Hence, Theorem 1 will be proved completely if we show that S is a reduced m-ring and that $S^{\#}$ is its extended ring with unit element $\mathbb{1}_0$.

This proof will be given in a number of steps.

(E) Let e be an idempotent of $R^{\#}$ and set $A = eRe$. 1) If $e \in R$, then $eR^{\#}e = A$. 2) If $e \notin R$, then $eR^{\#}e$ is the extended ring $A^{\#}$ of A with the unit element e.

Proof: If $e \in R$, then $eR^{\#}e = eRe$ by (B5). Suppose then $e \notin R$. The most general element x of $eR^{\#}e$ has the form $x = e(r + n\mathbb{1})e$ with $r \in R$, $n \in \mathbb{Z}$, and if we set $a = ere$,

$$x = a + ne \quad , \text{ with } a \in A, \ n \in \mathbb{Z}. \tag{17}$$

We only have to prove that the representation (17) of x is unique. If this was not so, we could find an $n_0 \in \mathbb{Z}$, $n_0 \neq 0$ with $n_0 e \in A = eRe \subseteq R$. However, if we set $e = r_1 + n_1 \mathbb{1}$ with $r_1 \in R$, $n_1 \in \mathbb{Z}$, then $e \notin R$ implies $n_1 \neq 0$. Thus, $n_0 e = n_0 r_1 + n_0 n_1 \mathbb{1} \notin R$, a contradiction.

(F) Let e be an idempotent of $R^{\#}$. Then $A = eRe$ is an m-ring.

Proof: Let X be an r-ideal of A and set $Y = XR^{\#}$. Then Y is an r-ideal of $R^{\#}$. Since $X \subseteq R$, we have $Y \subseteq R$. Thus, Y is an r-ideal of R. Moreover, since $X = Xe$, we find

$$Ye = XR^{\#}e = XeR^{\#}e .$$

If $e \in R$, then $eR^{\#}e = A$ and as X is an r-ideal of A and A has a unit element, $XeR^{\#}e = X$. If $e \notin R$, then $eR^{\#}e = A^{\#}$ by (E) and we still find $XeR^{\#}e = X$.

In either case, $Ye = X$. This shows that we have a one-to-one correspondence $X \longrightarrow Y$ of the set $\{X\}$ of r-ideals X of A into the set of r-ideals of R such that $Y = XR^{\#}$, $X = Ye$. If $X_1, X_2 \in \{X\}$ and $X_1 \longrightarrow Y_1$, $X_2 \longrightarrow Y_2$, we have $X_1 \subseteq X_2$ iff $Y_1 \subseteq Y_2$. It is now clear that the m-condition for r-ideals of R implies the m-condition for r-ideals of A and (F) is proved.

We may apply (E) and (F) with $e = 1_0$. Here, by (15), $e \notin R$ since $e_i \in R$ for $i > 0$, but $e_0 \notin R$. It is now clear that S is an m-ring and that $S^{\#}$ is the extended ring with the unit element 1_0.

Our next proposition is:

(G) Let e and e^* be two idempotents of $R^{\#}$ with $e \in R$. Assume that the $R^{\#}$-modules $U = eR^{\#} = eR$ and $U^* = e^*R^{\#}$ are indecomposable. Let c be an element of $eR^{\#}e^*$ and set $\theta = \mathcal{L}(c) \mid U^*$. Then either θ is an $R^{\#}$-isomorphism of U^* onto U, or $c \in \mathrm{Rad}(R)$ and θ maps U^* into $W = U \cap \mathrm{Rad}(R)$.

Proof: Since $e \in U$, U is a potent r-ideal and hence includes a minimal potent r-ideal $\widetilde{U}$. Now, Chapter IV, (R) shows that

$\tilde{U}$ is a component of U. Since U is indecomposable, we must have $\tilde{U} = U$, that is, U itself is minimal potent. It follows from Chapter IV (U) that U has the greatest proper submodule $W = U \cap \mathrm{Rad}(R)$.

For $c \in eR^{\#}e^*$, $\theta = \mathcal{L}(c) \mid U^* \in \mathrm{Hom}(U^*, U)$. If $c \notin \mathrm{Rad}(R)$, then $c \notin W$. Since θ maps $e^* \longrightarrow c$, we have $U^*\theta \not\subseteq W$. It follows that $U^*\theta = U$. Since U^* is also indecomposable, θ is an isomorphism by Chapter IV, (I*).

On the other hand, if $c \in \mathrm{Rad}(R)$, then $U^*\theta = cU^* \subseteq \mathrm{Rad}(R)$ and hence $U^*\theta \subseteq U \cap \mathrm{Rad}(R) = W$.

Proposition (G) is supplemented by the following remark which deals with the case $e \notin R$:

(G*) If $eR^{\#}$ is an indecomposable component of $R^{\#}$ and $e \notin R$, then $eR \subseteq$ Rad

Indeed, if $eR \not\subseteq \mathrm{Rad}(R)$, then eR would be a potent r-ideal of R and hence would include a minimal potent r-ideal $\tilde{U}$. Again, Chapter IV(R) would show that $\tilde{U}$ is a component of $eR^{\#}$. Since $eR^{\#}$ was indecomposable, this would mean $eR^{\#} = \tilde{U}$ and hence $e \in eR^{\#} \subseteq R$, a contradiction.

We show next that

(18) $\qquad e_iRe_j \subseteq \mathrm{Rad}(R)$, for $i \neq j$ and for $i = j = 0$.

If $i = 0$, then $e_0 \notin R$ and (18) is a consequence of (G*). If $i > 0$, apply (G) to $e = e_i$ and $e^* = e_j$. If $c \in eR^{\#}e^*$, and $\theta = \mathcal{L}(c) \mid U_j$, then either θ is an $R^{\#}$-isomorphism of U_j onto U_i or $c \in \mathrm{Rad}(R)$. For $i \neq j$, U_i

are not $R^{\#}$-isomorphic and we must have the second case. Thus, $e_iR^{\#}e_j \subseteq \mathrm{Rad}(R)$ for $i > 0$, $i \neq j$ and (18) is proved.

We recall that an idempotent e is termed indecomposable, if it cannot be written as sum of two orthogonal idempotents. This is so, iff $eR^{\#}$ is indecomposable. If $e \in R$, then $eR = eR^{\#}$ (cf. (B4)) and we see that indecomposability of e does not depend on whether e is considered as idempotent of $R^{\#}$ or of R (see also Problem 1). As an application of (G), we have

(H) If e is an indecomposable idempotent of R, the ring $P = eRe$ has the radical $P \cap \mathrm{Rad}(R)$ and $P/\mathrm{Rad}(P)$ is a skew field.

Proof: By (B5), $P = eRe = eR^{\#}e$. Set $Q = P \cap \mathrm{Rad}(R)$. It is clear that Q is an ideal of P. Since R is an m-ring, its radical is nilpotent and this implies that Q is nilpotent. Hence $Q \subseteq \mathrm{Rad}(P)$.

On the other hand, if $c \in P$, $c \notin Q$, then $c \notin \mathrm{Rad}(R)$ and (G) shows that $\mathfrak{L}(c) \mid eR^{\#}$ is an $R^{\#}$-isomorphism of $eR^{\#}$ onto $eR^{\#}$. It now follows from (C2) with $e = e^*$ that there exists an element $c^* \in eRe = P$ such that $cc^* = c^*c = e$. Since e is the unit element of P, this proves that every element $c \in P$ with $c \notin Q$ has an inverse c^* in P. Consequently, P/Q is a skew field. In particular, P/Q is semisimple and hence $Q \supseteq \mathrm{Rad}(P)$ (for instance by Chapter III (F)). Thus $Q = \mathrm{Rad}(P)$ and we are finished.

We complete now the proof of Theorem 1 by showing that S in (16) is a reduced ring. For $s \in S$, we have

$$s = 1_0 \, s \, 1_0 = \sum_{i,j=0}^{k} e_i \, s \, e_j$$

(cf. (15)). Now (18) yields

$$s \equiv \sum_{i=1}^{k} e_i s e_i \qquad \text{mod Rad}\,(R). \tag{19}$$

All terms appearing here belong to S. Thus, if we set $N_0 = S \cap \text{Rad}\,(R)$, the congruence (19) holds modulo the ideal N_0 of S. If $\lfloor x \rfloor$ denotes the residue class of $x (\text{mod } N_0)$, we can write our result in the form

$$\lfloor s \rfloor = \sum_{i=1}^{k} \lfloor e_i s e_i \rfloor \quad . \tag{20}$$

For fixed i, $1 \leqq i \leqq k$, set

$$T_i = \{ \lfloor e_i \, x \, e_i \rfloor \mid x \in S \}.$$

Then T_i is a subring of S/N_0 and (20) shows that $S/N_0 = \sum_{i=1}^{k} T_i$. Because of the orthogonality of $\{e_i\}$, $T_i T_j = (0)$ for $i \neq j$ and it follows that each T_i is an ideal of S/N_0. It is also seen easily that $\sum_{i=1}^{k} T_i$ is direct. Indeed, if $\sum_i t_i = 0$ with $t_i \in T_i$, multiplication with $\lfloor e_j \rfloor$ yields $t_j = 0$, $(j = 1, 2, \ldots, k)$. Thus

$$S/N_0 \approx \oplus \sum_{i=1}^{k} T_i \tag{21}$$

(cf. Chapter V, Section 1).

Set $P_i = e_i R e_i$. Since $e_i = e_i 1_0 = 1_0 e_i$, then $P_i = e_i 1_0 R 1_0 e_i =$ $e_i S e_i$. If we map $e_i s e_i \longrightarrow \lfloor e_i s e_i \rfloor$, we have a ring homomorphism of P_i onto T_i. Clearly, the kernel Q_i is given by $Q_i = P_i \cap \text{Rad}\,(R)$.

Now ($\underline{H}$) shows that $T_i \approx P_i/Q_i$ is a skew field. In particular, (21) shows that S/N_0 is semisimple and, by Chapter III, ($\underline{F}$), this implies $N_0 \supseteq \mathrm{Rad}\,(S)$. On the other hand, since $\mathrm{Rad}\,(R)$ is nilpotent, so is $N_0 = S \cap \mathrm{Rad}\,(R)$. Hence, $N_0 \subseteq \mathrm{Rad}\,(S)$, that is, $N_0 = \mathrm{Rad}\,(S)$. By (21) $S/\mathrm{Rad}\,(S)$ is isomorphic with a Cartesian sum of skew fields T_i. This proves that S is a reduced ring and we are finished.

3. Corollaries

We first prove ($\underline{A}$) Section 1. Assume then that R is an m-ring with unit element η. Since η is the only left unit element of R, it follows from Chapter IV, ($\underline{S}$**) that $\eta = 1 - e_0$. Hence $e_0 r = (1 - \eta) r = r - r = 0$ for $r \in R$. Similarly, $re_0 = 0$ for $r \in R$. Thus, $e_0 R e_j = (0)$ and $e_i R e_0 = (0)$. This means that, in all matrices (1*), we have $m_{\tau\omega} = 0$ if $\tau = (0, 1)$ or if $\omega = (0, 1)$. If we remove this row and column consisting of zeros from the matrices of M, we obtain the matrices of M_1 in (1). Moreover, S has the unit element $1_0 \eta 1_0$. Thus, ($\underline{A}$) is a consequence of ($\underline{A}$*).

If R is an m-ring, we shall call the ring S in (16) the *reduced ring of R*. Our uniqueness theorem ($\underline{Q}$) will show S is determined apart from isomorphism.

If we have a one-to-one correspondence $X \longrightarrow Y$ between the set $\{X\}$ of all ideals of a ring A and the set of all ideals $\{Y\}$ of a ring B, we speak of a *lattice isomorphism*, when the following condition holds: If $X_1 \longrightarrow Y_1$ and $X_2 \longrightarrow Y_2$, then $X_1 \subset X_2 \iff Y_1 \subset Y_2$. This implies

$X_1 \cap X_2 \longrightarrow Y_1 \cap Y_2$ and $X_1 + X_2 \longrightarrow Y_1 + Y_2$. Of course, a one-to-one correspondence $X \longrightarrow Y$ is called a multiplicative isomorphism, if $X_1 \longrightarrow Y_1$, $X_2 \longrightarrow Y_2$ implies $X_1X_2 \longrightarrow Y_1Y_2$.

(I) Theorem 2. If R is an m-ring and if S is its reduced ring, we have a one-to-one correspondence $H \longrightarrow L$ between the set $\{H\}$ of all ideals of R and the set $\{L\}$ of all ideals of S which is both a lattice isomorphism and a multiplicative isomorphism and which associates Rad (R) with Rad (S).

Remark: If S is identified with a subring of R as in (16), the correspondence $H \longrightarrow L$ can be defined by $L = H \cap S = 1_0 H 1_0$, $H = R^\# L R^\#$.

Proof: We use the same notation as in Section 2. If H is an ideal of R, set $L = 1_0 H 1_0 = H \cap S$, (cf. (B3)). As shown by (D), the ring isomorphism of R onto $M = M(S, \{e\}, \{q\})$ maps H onto the set $\tilde{H}$ of matrices $[m_{\tau\omega}] \in M$ with $m_{\tau\omega} \in H$. Since $m_{\tau\omega} \in S$, here $\tilde{H}$ is exactly the set of matrices in M with coefficients in L. This shows that H is uniquely determined by L and $H \longrightarrow L$ is a one-to-one mapping of the set $\{H\}$ into $\{L\}$.

Actually, $\{H\}$ is mapped onto $\{L\}$. Indeed, if L is an ideal of S, then $H = R^\# L R^\#$ is an ideal of $R^\#$. Since $L \subseteq S \subseteq R$, we have $H \subseteq R$ and H is an ideal of R. Moreover, as $L 1_0 = L = 1_0 L$, we find

$$1_0 H 1_0 = 1_0 R^\# L R^\# 1_0 = 1_0 R^\# 1_0 L 1_0 R^\# 1_0 = S^\# L S^\#.$$

Since L is an ideal of S, we have $S^\# L S^\# = L$. Thus, H is mapped on the given L.

Thus, our correspondence $H \longrightarrow L$ is described by $L = 1_0 H 1_0$, $H = R^\# L R^\#$. It is clear that it is a lattice isomorphism. Moreover, if

$L_1, L_2 \in \{L\}$, then $L_1 \mathbf{1}_0 = L_1$, $\mathbf{1}_0 L_2 = L_2$. Hence $L_1 R^\# L_2 = L_1 \mathbf{1}_0 R^\# \mathbf{1}_0 L_2$ $L_1 S^\# L_2 = L_1 L_2$. This implies

$$R^\# L_1 R^\# R^\# L_2 R^\# = R^\# L_1 L_2 R^\#$$

and we have a multiplicative isomorphism.

As another corollary of Theorem 1, we have

(J) An m-ring R is reduced, if no two components in a full decomposition of $R^\#$ are $R^\#$-isomorphic.

Proof: If no two components of $R^\#$ in the full decomposition (4) of $R^\#$ are $R^\#$-isomorphic, then all q_i are 1. It follows from (5) and (15) that $\mathbf{1} = \mathbf{1}_0$. Then $R = S$ by (16) and we know that S is reduced.

A converse of (J) will be given in Section 4.

4. Properties of reduced rings.

Let R be a reduced ring of height n. Then $T = R/\mathrm{Rad}\,(R)$ is a direct sum of n ideals T_j such that each T_j is a skew field. We write

$$(22) \qquad R/\mathrm{Rad}\,(R\} = T = \oplus \sum_{j=1}^{n} T_j \,.$$

identifying the direct sum $\bullet \sum_j T_j$ with the Cartesian sum $\oplus \sum_j T_j$. The unit element of T_j will be denoted by $\mathbf{1}_j$.

Let ν be the natural homomorphism $r \longrightarrow \lfloor r \rfloor$ of R onto T. We shall say that an idempotent e of R is associated with T_j in (22), if $e\nu = \mathbf{1}_j$.

(K) Let R be a reduced ring of height n and set $R/\mathrm{Rad}\,(R) = T =$

$\oplus \sum_{j=1}^{n} T_j$ where the T_j are skew fields.

1) If $\{h_1, h_2, \ldots, h_m\}$ is a system of m orthogonal idempotents of R, then $m \leqq n$.

2) If $m = n$, the h_i can be so labelled that h_i is associated with T_i for $i = 1, 2, \ldots, n$. Moreover, if $R^{\#}$ is the extended ring with unit element 1 and if we set $h_0 = 1 - \sum_{i=1}^{n} h_i$, then $1 = \sum_{i=0}^{n} h_i$ is a resolution of 1 into indecomposable orthogonal idempotents.

Proof: 1) We note first that 1_j is the only idempotent of T_j for if $t^2 = t$ with $t \in T_j$, then $(t - 1_j)t = 0$ and hence $t = 1_j$ or $t = 0$. It follows that the most general idempotent of $\oplus \sum_j T_j$ has the form $\sum_{j \in B} 1_j$ where B is a non-empty subset of $\{1, 2, \ldots, n\}$.

Clearly, $\mathcal{U}$ maps $\{h_i\}$ on a system of orthogonal idempotents $\{h_i \mathcal{U}\}$ and if we set

$$h_i \mathcal{U} = \lfloor h_i \rfloor = \sum_{j \in B} 1_j ,$$

the subsets B_i of $\{1, 2, \ldots, n\}$ must be disjoint. This implies $m \leqq n$.

2) Assume now $m = n$. Here each B_j consists of one element and if the $\{h_j\}$ are labelled suitably, we have $B_i = \{i\}$. Then $h_i \mathcal{U} = 1_i$ is associated with T_i for $i = 1, 2, \ldots, n$.

If we set $h_0 = 1 - \sum_{i=1}^{n} h_i$, then $h_0 \neq 0$, since $\sum_{i=1}^{n} h_i \in R$ and $1 \notin R$. We now see that $\{h_0, h_1, \ldots, h_n\}$ is a system of $n + 1$ orthogonal idempotents. If some h_j was a sum $h_j = h_j' + h_j''$ of two orthogonal idempotents and if we replace h_j in our system by the two idempotents h_j', h_j'', we show easily that we obtain a system of $n + 2$ orthogonal idempotents. On account of (B6), $n + 1$ of these would lie in R.

However, we have seen in 1) that this is impossible. Thus, each h_i is indecomposable as we had to show.

Assume now that the reduced ring R is an m-ring. We use the same notation as in Section 2, in particular, in (4) and (6). If $i > 0$, $e_i^{(\lambda)} \in R$ and $U_i^{(\lambda)} = e_i^{(\lambda)}R$ has the greatest proper submodule $W_i^{(\lambda)} = U_i^{(\lambda)} \cap \mathrm{Rad}\,(R)$. If $\mathcal{A}$ has the same significance as above, then $W_i^{(\lambda)}\mathcal{A} = (0)$ while $e_i^{(\lambda)} \notin \mathrm{Rad}\,(R)$ implies $U_i^{(\lambda)}\mathcal{A} \neq (0)$. It follows that $U_i^{(\lambda)}\mathcal{A}$ is a simple submodule of T. Clearly, the only simple submodules of T in (22) are $T_1, T_2, \ldots, T_n$. Thus, $U_i^{(\lambda)}\mathcal{A} = T_j$ for some j. In particular, the ring homomorphism $\mathcal{A}$ must map $e_i^{(\lambda)}$ on the (only) idempotent 1_j of T_j. Since $e_i^{(\lambda)}e_j^{(\mu)} = 0$ for $e_i^{(\lambda)} \neq e_j^{(\mu)}$, $e_j^{(\mu)}$ cannot map on 1_j too. Hence different components $U_i^{(\lambda)}$ with $i > 0$ map on different T_j.

Consider two of the ideals T_j and T_g in (22) with $g \neq j$. Any $\theta \in \mathrm{Hom}_T(T_g, T_j)$ maps T_g onto $T_jT_g = (0)$. Thus, T_g and T_j are not T-isomorphic. Now $\mathcal{A}$ maps R-isomorphic components $U_i^{(\lambda)}$ and $U_i^{(\mu)}$ on T-isomorphic images. It follows that $U_i^{(\mu)}\mathcal{A} = U_i^{(\lambda)}\mathcal{A} = T_j$ and we have seen that this implies $U_i^{(\lambda)} = U_i^{(\mu)}$. It follows that $q_i = 1$ for $i > 0$. As $q_0 = 1$, all the q_i in (4) are 1 if R is reduced. We now see that the "if" in $(\underline{J})$ can be replaced by "iff". Thus,

$(\underline{J}^*)$ An m-ring R is reduced, iff no two components in a full decomposition of $R^{\#}$ are $R^{\#}$-isomorphic.

If follows from (4), (6), and $q_i = 1$ that

$$R = (U_0 \cap R) \dot{+} U_1 \dot{+} \dots \dot{+} U_k .$$

Here, $U_0 \cap R = e_0R \subseteq \mathrm{Rad}(R)$ (By (B2) and (G*)). Thus, $(U_0 \cap R)\mathcal{V} = (0)$. Since $R\mathcal{V} = T$, it is now obvious that each T_j is the image of some U_i. Hence $k = n$ and for suitable choice of notation, $U_i\mathcal{V} = T_i$ for $i = 1, 2, \dots, n$.

In Chapter IV, Section 5, the number k in (4) was called the height of the m-ring R. In Definition 1, we introduced n as the height of the reduced ring R. We now see that for reduced m-rings, both definitions coincide. Moreover, we have shown

(L) If R is a reduced m-ring of height n, a resolution $1 = \sum_i e_i$ of 1 into indecomposable orthogonal idempotents consists of $n + 1$ idempotents. These can be labelled such that $e_0 \notin R$ and that each e_i is associated with T_i.

We also mention

(M) An m-ring R and its reduced m-ring S have the same height k.

Indeed by the definition in Chapter IV, Section 5, the height of the m-ring R in (4) is k and (21) shows that S has the same height k.

5. Formal properties of checkered matrix rings.

Let S be a reduced m-ring of height k, let $\{e\}$ be a system of k orthogonal idempotents of S and let $\{q\}$ be a system of k natural integers. We may then form the checkered matrix ring $M = M(S, \{e\}, \{q\})$.

As in Definition 2*, we set $q_0 = 1$, $e_0 = 1_0 - \sum_{i=1}^{k} e_i$ where 1_0 is the unit element of the extended ring $S^{\#}$. By ($\underline{K}$), $1_0 = \sum_{i=0}^{k} e_i$ is a resolution of 1_0 into indecomposable orthogonal idempotents of $S^{\#}$. Again, let C denote the set of all ordered pairs $\tau = (i, \lambda)$ with $0 \leqq i \leqq k$, $1 \leqq \lambda \leqq q_i$ and set $e_\tau = e_i$ for $\tau = (1, \lambda) \in C$.

Let $M^{\#}$ denote the set of all matrices

$$[m_{\tau\omega}];\ \tau, \omega \in C\ ;\begin{cases} \tau \text{ row index} \\ \omega \text{ column index} \end{cases} \tag{23}$$

whose coefficients satisfy the conditions

$$m_{\tau\omega} \in e_\tau S^{\#} e_\omega \quad \text{(for all } \tau, \omega \in C). \tag{24}$$

It is clear that $M^{\#}$ is a ring. If we replace the set $e_\tau S^{\#} e_\omega$ by $e_\tau S e_\omega$, we obtain the checkered matrix ring M. Actually, by ($\underline{B}$5), $e_\tau S^{\#} e_\omega = e_\tau S e_\omega$ except for $\tau = \omega = (0, 1)$. Thus, the only difference between M and $M^{\#}$ lies in the conditions for the one coefficient $m_{\tau\tau}$ with $\tau = (0, 1)$. We shall justify our notation below by showing that $M^{\#}$ is the extended ring belonging to M. Clearly, M is an ideal of $M^{\#}$.

If α and β are two elements of C and if $x_{\alpha\beta} \in e_\alpha S^{\#} e_\beta$, we can form the element $[m_{\tau\omega}]$ of $M^{\#}$ for which $m_{\alpha\beta} = x_{\alpha\beta}$ while all other $m_{\tau\omega}$ vanish. This element will be denoted by $\tilde{x}_{\alpha\beta}$. The general element $[m_{\tau\omega}]$ of $M^{\#}$ can then be written in the form

$$[m_{\tau\omega}] = \sum_{\tau, \omega \in C} \tilde{m}_{\tau\omega} \tag{25}$$

and the representation of an element of $M^{\#}$ as such a sum is unique. For

$\alpha, \beta, \gamma, \delta \in C$ and $x \in e_\alpha S^\# e_\beta$ and $y \in e_\gamma S^\# e_\delta$, it is seen at once that

$$(26) \qquad \tilde{x}_{\alpha\beta}\tilde{y}_{\gamma\delta} = \begin{cases} 0 & \text{for } \beta \neq \gamma \\ (\widetilde{xy})_{\alpha\delta} & \text{for } \beta \neq \gamma \end{cases} .$$

Some special cases are of interest. First, take $\alpha = (i, \lambda)$, $\beta = (i, \mu)$ with the same i. Then $e_i \in e_\alpha S^\# e_\beta$. Set

$$e_i^{(\lambda\mu)} = (\tilde{e}_i)_{\alpha\beta} \qquad \text{for } \alpha = (i, \lambda), \ \beta = (i, \mu) \ .$$

We write $e_i^{(\lambda)}$ for $e_i^{(\lambda\lambda)}$. It follows from (26) that

$$(27) \qquad e_i^{(\lambda\mu)} e_i^{(\mu\rho)} = e_i^{(\lambda\rho)} \ ,$$

$$(28) \qquad e_i^{(\lambda\mu)} e_j^{(\nu\rho)} = 0 \quad \text{for } i \neq j \text{ or } \mu \neq \nu.$$

In particular, $\{e_i^{(\lambda)}\}$ with $(i, \lambda) \in C$ is a system of orthogonal idempotents. Moreover, (26) yields

$$(29) \qquad e_i^{(\lambda)} \sum_{\tau, \omega \in C} \tilde{m}_{\tau\omega} = \sum_{\omega \in C} \tilde{m}_{\alpha\omega} \quad \text{for } \alpha = (i, \lambda) ;$$

$$(30) \qquad e_i^{(\lambda)} \Big(\sum_{\tau, \omega \in C} \tilde{m}_{\tau\omega}\Big) e_j^{(\mu)} = \tilde{m}_{\alpha\beta} \quad \text{for } \alpha = (i, \lambda), \ \beta = (j, \mu) .$$

It follows from (29) and (30) that

$$(31) \qquad 1 = \sum_{i=0}^{k} \sum_{\lambda=1}^{q_i} e_i^{(\lambda)}$$

is a unit element of $M^\#$. We can prove now that $M^\#$ is the extended ring of M with the unit element $\mathbf{1}$. Let α denote the fixed pair $(0,1) \in C$. A remark above shows that $\tilde{m}_{\tau\omega} \in M$ except for $\tau = \omega = \alpha$. In particular, $e_i^{(\lambda)} \in M$ for $i > 0$ and $\mathbf{1} \equiv e_0^{(1)}$ (mod M) by (31). Moreover, it follows from (25) that every element ξ of $M^{\#}$ is congruent (mod M) to an element $\tilde{m}_{\alpha\alpha}$ where $m_{\alpha\alpha}$ is an element of $e_0 S^{\#} e_0$. Set $m_{\alpha\alpha} = e_0(t + n\mathbf{1})e_0$ where $t \in S$, $n \in \mathbb{Z}$. Then $m_{\alpha\alpha} = s + ne_0$ with $s = e_0te_0 \in S$ and $\tilde{m}_{\alpha\alpha} = \tilde{s}_{\alpha\alpha} + n(\tilde{e}_0)_{\alpha\alpha} = \tilde{s}_{\alpha\alpha} + ne_0^{(1)}$. Since $\tilde{s}_{\alpha\alpha} \in M$, we find $\xi \equiv ne_0^{(1)} \equiv n\mathbf{1}$ (mod M). Thus, ξ has the form $\xi = m + n\mathbf{1}$ with $m \in M$, $n \in \mathbb{Z}$. We will be finished when we can show that $n\mathbf{1} \notin M$ for $n \in \mathbb{Z}$, $n \neq 0$. Now (31) shows that if we set $n\mathbf{1} = [m_{\tau\omega}]$ then $m_{\alpha\alpha} = ne_0 = n(\mathbf{1}_0 - \sum_{i=1}^{k} e_i)$. Since $e_i \in S$ for $i > 0$ and $n\mathbf{1}_0 \notin S$ for $n \neq 0$, indeed $m_{\alpha\alpha} \notin S$ and $n\mathbf{1} \notin M$. This justifies the use of the symbol $M^{\#}$ above.

If x is an element of $S^{\#}$, set $x_{ij} = e_ixe_j$. Then

$$x = \mathbf{1}_0 x \mathbf{1}_0 = \sum_{i=0}^{k} e_i x \sum_{j=0}^{k} e_j = \sum_{i,j} x_{ij} .$$

We wish to identify x with an element of $M^{\#}$. If $\tau = (i,1)$, $\omega = (j,1)$, the element $x_{ij} \in e_i S^{\#} e_j = e_\tau S^{\#} e_\omega$ is to be identified with the element $(\tilde{x}_{ij})_{\tau\omega}$ and x with the corresponding sum $\sum_{i,j=0}^{k} (\tilde{x}_{ij})_{\tau\omega}$. If we write for a moment $x\chi$ for this sum, it is clear that the mapping χ is an additive isomorphism of $S^{\#}$ into $M^{\#}$. If also $y \in S^{\#}$, then

$$xy = \sum_i e_i \, x \sum_\nu e_\nu \, y \sum_j e_j = \sum_{i,j,\nu} e_i x e_\nu e_\nu y e_j$$

and it follows from (26) that $(xy)\chi = (x\chi)(y\chi)$. Hence χ is a ring isomorphism and the identification of $x\chi$ with x is possible. Then $S^{\#}$ is a subring of $M^{\#}$

and S a subring of M.

In particular, e_i is identified with $e_i^{(1)}$ whence

$$(32) \qquad 1_0 = \sum_{i=0}^{k} e_i^{(1)} .$$

We also note that

$$(33) \qquad S^{\#} = 1_0 M^{\#} 1_0 , \quad S = 1_0 M 1_0 .$$

Indeed, since $S^{\#}$ has the unit element 1_0, $S^{\#} \subseteq 1_0 M^{\#} 1_0$ and $S \subseteq 1_0 M 1_0$. On the other hand, it follows from (32) that each $\xi \in 1_0 M^{\#} 1_0$ is a sum of elements $\tilde{x}_{\tau\omega}$ with $\tau = (i, 1)$, $\omega = (j, 1)$ and $x_{\tau\omega} \in e_i S e_j$. Then $\tilde{x}_{\tau\omega} \in S^{\#}$ and hence $\xi \in S^{\#}$. Moreover, if $\xi \in 1_0 M 1_0$, all $x_{\tau\omega}$ belong to $e_i S e_j$ and we find $\xi \in S$. Thus, $1_0 M^{\#} 1_0 \subseteq S^{\#}$, $1_0 M 1_0 \subseteq S$ and (33) holds.

Suppose that $\tau = (i, \lambda)$, $\omega = (j, \mu)$, $\omega = (j, \mu)$ and that $x \in e_\tau S^{\#} e_\omega = e_i S^{\#} e_j$. Take $\alpha = (i, 1)$, $\beta = (j, 1)$. It follows from (26) that $(\tilde{e}_i)_{\tau\alpha} \tilde{x}_{\alpha\beta} (\tilde{e}_j)_{\beta\omega} = \tilde{x}_{\tau\omega}$, that is, $e_i^{(\lambda 1)} \tilde{x}_{\alpha\beta} e_j^{(1\mu)} = \tilde{x}_{\tau\omega}$. Here, $\tilde{x}_{\alpha\beta} \in S^{\#}$ and using (25), we see that the ring $M^{\#}$ is generated by the subring $S^{\#}$ and the set $\{e_j^{(\lambda\mu)}\}$ with $0 \leqq j \leqq k$; $1 \leqq \lambda, \mu \leqq q_j$.

We come to the converse of Theorem 1.

(N) Theorem 3. If S is a reduced m-ring, the checkered matrix ring $M = M(S, \{e\}, \{q\})$ is an m-ring.

Proof: It follows from (31) that

$$M = \cdot \sum_{i=0}^{k} \cdot \sum_{\lambda=1}^{q_i} e_i^{(\lambda)} M.$$

It will be sufficient to prove the descending chain condition for the submodules of each fixed $e_i^{(\lambda)}M$, cf. Section 5 (I) of the Appendix.

Let $\alpha = (i, \lambda)$. Let X be a submodule of $e_i^{(\lambda)}M$. If $\omega = (j, \mu) \in C$, let X_ω denote the set of all elements $z \in e_\alpha S e_\omega$ for which $\tilde{z}_{\alpha\omega} \in X$. It follows from (29) that every element of $X \subseteq e_i^{(\lambda)} M$ has the form $x = \sum_{\omega \in C} \tilde{m}_{\alpha\omega}$ with $m_{\alpha\omega} \in e_\alpha M e_\omega$. By (30), $xe_j^{(\mu)} = \tilde{m}_{\alpha\omega}$ and since $xe_j^{(\mu)} \in X$, $\tilde{m}_{\alpha\omega} \in X$. Hence $m_{\alpha\omega} \in X_\omega$. Thus, X consists exactly of the sums $\sum_{\omega \in C} \tilde{m}_{\alpha\omega}$ with $m_{\alpha\omega} \in X_\omega$. This proves that X is uniquely determined by the system $\{X_\omega\}$ of sets X_ω with $\omega \in C$.

If $x \in X_\omega \subseteq e_\alpha S e_\omega$ and $y \in e_\omega S^{\#} e_\omega$, then by (26) $(\widetilde{xy})_{\alpha\omega} = \tilde{x}_{\alpha\omega}\tilde{y}_{\omega\omega}$ and since $\tilde{x}_{\alpha\omega} \in X$, we have $(\widetilde{xy})_{\alpha\omega} \in X$ and hence $xy \in X_\omega$. This shows that $X_\omega(e_\omega S^{\#} e_\omega) \subseteq X_\omega$. Since $X_\omega e_\omega = X_\omega$, we must have equality and find

$$X_\omega S^{\#} e_\omega = X_\omega. \tag{34}$$

Set Set $Y_\omega = X_\omega S^{\#}$. Since $X_\omega \subseteq S$, it is clear that Y_ω is an r-ideal of S. Thus, for every submodule X of $e_i^{(\lambda)}M$, we have a system $\{Y_\omega\}$ of r-ideals of S with ω ranging over C. Suppose now that

$$X^{(1)} \supseteq X^{(2)} \supseteq \dots \supseteq X^{(n)} \supseteq \dots \tag{35}$$

is a descending sequence of submodules of $e_i^{(\lambda)}M$. Let $\{Y_\omega^{(n)}\}$ denote the system of r– ideals of S associated with $X^{(n)}$. It follows from (35) that

$$Y_\omega^{(1)} \supseteq Y_\omega^{(2)} \supseteq \ldots \supseteq Y_\omega^{(n)} \supseteq \ldots$$

for each $\omega \in C$. Since S is an m-ring and since C is a finite set, we can find an index N such that $Y_\omega^{(n)} = Y_\omega^{(N)}$ for $n \geqq N$ and all ω. Hence, $X_\omega^{(n)}S^\# = X_\omega^{(N)}S^\#$ and, by (34), $X_\omega^{(n)} = X_\omega^{(N)}$ for these ω, n. Since we have seen above that X is determined by the system $\{X_\omega\}$, this proves $X^{(n)} = X^{(N)}$ for all $n \geqq N$. Hence the descending chain condition holds and (N) is proved.

The resolution of 1 in (31) yields the decomposition

$$(36) \qquad M^\# = \cdot\sum_{i=0}^{k} \cdot\sum_{\lambda=1}^{q_i} e_i^{(\lambda)}M^\# .$$

Here, $e_i^{(\lambda)} \in M$ for $i > 0$, $e_0^{(1)} \notin M$. We show next that each $e_i^{(\lambda)}$ is indecomposable. Indeed, suppose that $e_i^{(\lambda)} = h_1 + h_2$ where h_1 and h_2 are orthogonal idempotents. Then $e_i^{(\lambda)}h_1 = (h_1 + h_2)h_1 = h_1$. Similarly, $h_1e_i^{(\lambda)} = h_1$. Thus, $h_1 = e_i^{(\lambda)}h_1e_i^{(\lambda)}$ and (30) shows that h_1 has the form $h_1 = \tilde{x}_{\alpha\alpha}$ with $\alpha = (i,\lambda)$ and $x \in e_iS^\#e_i$. Similarly, $h_2 = \tilde{y}_{\alpha\alpha}$ with $y \in e_iS^\#e_i$. It follows now that $e_i = x + y$ and that x and y are orthogonal idempotents of $S^\#$. Since e_i is indecomposable in $S^\#$, this is impossible and $e_i^{(\lambda)}$ is indecomposable in $M^\#$.

Finally, we show that $e_i^{(\lambda)}M^\#$ and $e_j^{(\mu)}M^\#$ are $M^\#$-isomorphic, iff $i = j$. Indeed, if $i = j$, take $e = e_i^{(\lambda)}$, $e^* = e_i^{(\mu)}$, $c = e_i^{(\lambda\mu)}$,

$c^* = e_i^{(\mu\lambda)}$. It follows from (27) that the conditions of $(\underline{C}2)$ are satisfied and $e_i^{(\lambda)} M^\#$ and $e_j^{(\mu)} M^\#$ are $M^\#$-isomorphic.

On the other hand, assume that $e_i^{(\lambda)} M^\#$ and $e_j^{(\mu)} M^\#$ are $M^\#$-isomorphic. By $(\underline{C}2)$, there exist elements $c \in e_i^{(\lambda)} M^\# e_j^{(\mu)}$, $c^* \in e_j^{(\mu)} M^\# e_i^{(\lambda)}$ with $cc^* = e_i^{(\lambda)}$, $c^*c = e_j^{(\mu)}$. If $\alpha = (i, \lambda)$, $\beta = (j, \mu)$, (30) shows that we may set $c = \tilde{x}_{\alpha\beta}$, $c^* = \tilde{y}_{\beta\alpha}$ with $x \in e_i S^\# e_j$, $y \in e_j S^\# e_i$. Then, $\tilde{x}_{\alpha\beta}\tilde{y}_{\beta\alpha} = e_i^{(\lambda)} = (\tilde{e}_i)_{\alpha\alpha}$ and, by (26), $xy = e_i$. If $i \neq j$, it follows from $(\underline{G})$, $(\underline{G}^*)$ that $e_i S^\# e_j \subseteq \mathrm{Rad}(S)$, since $e_i S^\#$ and $e_j S^\#$ are not $S^\#$-isomorphic, cf. $(\underline{J}^*)$, p. 177. Hence $x \in \mathrm{Rad}(S^\#)$: and $xy = e_i$ is impossible. Hence $e_i^{(\lambda)} M^\# \not\cong e_j^{(\mu)} M^\#$ for $i \neq j$.

Thus, (36) is a full decomposition of M and the notation is analogous to that in (4).

It can now be seen easily that S is actually the reduced ring belonging to M. This is also an immediate consequence of the uniqueness theorem below.

6. Uniqueness.

Let R be a ring. By an automorphism θ of R, we mean a ring-isomorphism of R onto itself. Suppose that R has a unit element and let r be an element of R which has an inverse. Let J(r) be the mapping of R defined by

$$x \longrightarrow r^{-1}xr .$$

Clearly, J(r) is an automorphism of R. Automorphisms of this type are called inner automorphisms. It is clear that J(r) maps each ideal of R onto itself. We may now define inner automorphisms for rings R without unity element. We simply take inner automorphisms $J(r)$ of the extended ring $R^{\#}$ and restrict $J(r)$ to R. If we set $r = r + n\mathbf{1}$ and $r^{-1} = r_0' + n'\mathbf{1}$ with $r_0, r_0' \in R$ and $n, n' \in \mathbb{Z}$, we find $nn' = 1$, that is, $n = n' = \pm 1$. After replacing r by $-r$ if necessary, we see that an inner automorphism of R is a mapping of the form

$$x \longrightarrow x + r_0'x + xr_0 + r_0'xr_0$$

where r_0 and r_0' are quasi-inverse to each other. If R itself has a unit element, the new definition of inner automorphisms coincides with the old one.

The automorphisms of a ring R form a group under the composition of mappings and the inner automorphisms form a subgroup which is easily seen to be normal.

We first prove a proposition which supplements the results of Chapter IV.

(Q) Let R be an m-ring with the extended ring $R^{\#}$ and suppose that

$$R^{*} = \cdot\sum_{i=0}^{n} U_i = \cdot\sum_{j=0}^{m} V_j$$

are two decompositions into indecomposable components. Then $n = m$ and the V_j can be labelled such that U_i is $R^{\#}$-isomorphic with V_i for $i = 0, 1, 2, \ldots, n$. If this is done (in any possible way), there exists an inner automorphism φ of R^{*} which maps each U_i onto V_i.

Proof: 1) Let $\mathbf{1} = \sum_{i=0}^{n} e_i = \sum_{j=0}^{m} e^*_j$ with $e_i \in U_i$, $e^*_j \in V_j$ be the resolutions of $\mathbf{1}$ into orthogonal idempotents. We may choose our notation such that $e_i \in R$ for $i > 0$, cf. ($\underline{B}$6). Take $i > 0$ and let θ be an $R^{\#}$-endomorphism of $U_i = e_i R^{\#}$. It follows from ($\underline{G}$) that either θ is an $R^{\#}$-isomorphism of U_i or that θ has the form $\theta = \mathcal{L}(c) | U_i$ with $c \in \mathrm{Rad}\,(R)$. In the latter case, θ is nilpotent, since $\mathrm{Rad}\,(R)$ is nilpotent. Thus, in the terminology of Section 9 of the Appendix, the $R^{\#}$-groups U_i with $i > 0$ are Fitting groups. As shown in the Appendix Section 9, then the Krull-Schmidt Theorem applies to the two decompositions of the module $R^{\#}$. It follows that $m = n$ and that the V_i may be labelled such that each U_i is $R^{\#}$-isomorphic with V_i, $i = 0, 1, \ldots, n$.

If this is so, ($\underline{C}$2) shows that there exist elements $c_i \in e_i R^{\#} e^*_i$, $c^*_i \in e^*_i R^{\#} e_i$ with

(37) $$c_i c^*_i = e_i, \quad c^*_i c_i = e^*_i,$$

$(i = 0, 1, \ldots, n)$. Then $c^*_j e_j = c^*_j$, $e_i c_i = c_i$ and as $e_j e_i = 0$ for $i \neq j$, we have $c^*_j c_i = 0$ for $i \neq j$. Similarly, $c_i c^*_j = 0$ for $i \neq j$. If we set

$$r = \sum_{i=0}^{n} c_i, \quad r^* = \sum_{j=0}^{n} c^*_j,$$

it follows from (37) that $rr^* = 1 = r^*r$. Thus, r^* is the inverse r^{-1} of r. Moreover, for $0 \leq \nu \leq k$, $r^{-1} e_\nu r = \sum_{j,i} c^*_j e_\nu c_i = \sum_j c^*_j e_j c_\nu \sum_i e_i c_i = c^*_\nu c_\nu$ and (37) shows that the inner automorphism $\varphi = J(r)$ of $R^{\#}$ maps $e_\nu \longrightarrow e^*_\nu$ and hence $U_\nu = e_\nu R^{\#}$ onto $V_\nu = e^*_\nu R^{\#}$.

Remark: If $U_0 \not\subseteq R$ as above, then automatically $U_0\varphi \not\subseteq R$.

As a first application of (Q), we prove

(P) Let S be a reduced ring of height k, say

$$S/\mathrm{Rad}\,(S) = \oplus \sum_{i=1}^{k} T_i \quad ,$$

where the T_i are skew fields. Let $\{e_i\}$ and $\{e^*_i\}$ be two systems of orthogonal idempotents and choose the notation such that e_i and e^*_i are associated with T_i for $1 \leqq i \leqq k$. If $\{q_i\}$ is a system of k natural integers, we have a ring isomorphism

$$M(S, \{e_i\}, \{q_i\}) \approx M(S, \{e^*_i\}, \{q_i\}) .$$

Proof: By (Q), there exists an inner automorphism $\varphi = J(s)$ which maps the system $\{e_i\}$ onto $\{e^*_i\}$. Let $\lfloor x \rfloor$ again denote the residue class of $x \in S$ (mod Rad (S)). Since e_j is associated with T_j, $\lfloor e_j \rfloor = \mathbf{1}_j$. Hence

$$\lfloor e_j\varphi \rfloor = \lfloor s^{-1} e_j s \rfloor = \lfloor s \rfloor^{-1} \mathbf{1}_j \lfloor s \rfloor = \mathbf{1}_j .$$

Thus, $e_j\varphi$ is associated with T_j and as $e_j\varphi \in \{e^*_i\}$, we must have $e_j\varphi = e^*_j$.

Let $[\varphi]$ denote the mapping of $M = M(S, \{e\}, \{q_i\})$ obtained by applying φ to each coefficient of each element $[m_{\tau\omega}] \in M$. Clearly, $[\varphi]$ is an isomorphism of M onto $M(S, \{e^*\}, \{q_i\})$.

Our result shows that if isomorphic rings are considered as equal, the checkered matrix ring $M(S, \{e\}, \{q\})$ depends only on S and not on the system $\{e\}$. We then consider the degree q_i as associated with the skew field T_i .

As our next application of (Q) , we prove the uniqueness theorem.

(Q) Theorem 4. Let S be a reduced m-ring of height k, $\{e\}$ a system of k orthogonal idempotents of S , and $\{q\}$ a system of k degrees. Similarly, let $\overline{S}$ be a reduced ring of height $\overline{k}$, $\{\overline{e}\}$ a system of $\overline{k}$ orthogonal idempotents, and $\{\overline{q}\}$ a system of $\overline{k}$ degrees. If there exists a ring isomorphism θ of $\overline{M} = M(\overline{S}, \{\overline{e}\}, \{\overline{q}\})$ onto $M = M(S,\{e\},\{q\})$, then S and $\overline{S}$ are isomorphic and $k = \overline{k}$. If $\{\overline{e}\}$ is labelled suitably, there exists a ring isomorphism ψ of $\overline{S}$ onto S such that $\overline{e}_i\psi = e_i$, $\overline{q}_i = q_i$ for $i = 0, 1, 2, \ldots, k$.

Proof: The automorphism θ can be extended to an isomorphism of the extended ring $\overline{M}^{\#}$ onto $\overline{M}^{\#}$. This extension will be denoted by θ too. Take now the analogue of (36) for $\overline{M}^{\#}$ and apply θ . We then have a formula

$$M^{\#} = \cdot\sum_{i=0}^{\overline{k}} \cdot\sum_{\lambda=1}^{\overline{q}_i} (\overline{e}_i^{(\lambda)}\theta)\, M^{\#} . \tag{38}$$

Here, each $(\overline{e}_i^{(\lambda)}\theta)M^{\#}$ is an indecomposable component of $M^{\#}$. On the other hand, by (36)

$$M^{\#} = \cdot\sum_{i=0}^{k} \cdot\sum_{\lambda=1}^{q_i} e_i^{(\lambda)}M^{\#} . \tag{39}$$

It now follows from (Q) that there exists an inner automorphism of $M^{\#}$ which maps each $(\overline{e}_i^{(\lambda)}\theta)M^{\#}$ onto some $e_j^{(\mu)}M^{\#}$. Since $M^{\#}$ -

isomorphic components in (38) must map onto $M^\#$-isomorphic components in (39), it follows that $k = \bar{k}$ and that $\{\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_k\}$ can be arranged such that $(\bar{e}_i^{(1)}\theta)M^\#$ is $M^\#$-isomorphic with $e_i^{(1)}M^\#$ for $i = 0, 1, \ldots, k$. Then $q_i = \bar{q}_i$ and (Q) shows that there exists an inner automorphism φ of $M^\#$ such that $\bar{e}_i^{(\lambda)}\theta\varphi = e_i^{(\lambda)}$ for all i, λ. If we replace θ by $\theta\varphi$, we see that we may assume

$$(40) \qquad \bar{e}_i^{(\lambda)}\theta = e_i^{(\lambda)} \quad \text{for all } i, \lambda.$$

Set $1_0 = \sum_i e_i^{(1)}$ as in (32) and $\bar{1}_0 = \sum_i \bar{e}_i^{(1)}$, then $\bar{1}_0\theta = 1_0$. By (33), we have $S = 1_0 M 1_0$ and similarly $\bar{S} = \bar{1}_0 M \bar{1}_0$. It is now clear that $\theta \mid \bar{S}$ is an isomorphism of $\bar{S}$ onto S which maps $\bar{e}_i$ onto e_i.

7. Automorphisms of checkered matrix rings.

Let S be a reduced m-ring of height k and let $\{e\}$ be a system of k orthogonal idempotents of S. If ψ is an automorphism of S which leaves all e_i fixed, we obtain an automorphism $[\psi]$ of the checkered matrix ring $M = M(S, \{e\}, \{q\})$ by applying ψ to each coefficient of each $[m_{\tau\omega}] \in M$. We call $[\psi]$ the automorphism of M produced by the automorphism ψ of S.

(R) Theorem 5. Let S be a reduced m-ring and let $M = M(S, \{e\}, \{q\})$ be a checkered matrix ring. If θ is an automorphism of M, there exists an automorphism ψ of S which leaves every e_i fixed and such that θ is the product $\theta = [\psi]\varphi$ of the automorphism $[\psi]$ of M

produced by ψ and an inner automorphism φ of M.

Proof: We use the same method as in the proof of (Q) taking $M^{\#} = M$. After replacing θ by a produce $\theta\varphi_0$ of θ with a suitable inner automorphism φ_0 of M, we may assume that

$$e_i^{(\lambda)}\theta = e_i^{(\lambda)} \quad \text{for all } i, \lambda . \tag{41}$$

It suffices to prove (R) for the new θ. Again (41) implies $1_0\theta = 1_0$ and hence $\psi = \theta | S^{\#}$ is an automorphism of $S^{\#} = 1_0 M^{\#} 1_0$. Since $e_i\psi = e_i$ for all i, ψ produces an automorphism $[\psi]$ of $M^{\#}$. Then $[\psi]^{-1}\theta = \varphi$ is an automorphism of $M^{\#}$ which leaves every $s \in S^{\#}$ and all $e_i^{(\lambda)}$ fixed. We show that this implies that φ is inner. Set

$$r' = \sum_{(i,\lambda)\in C} (e_i^{(\lambda 1)}\varphi)e_i^{(1\lambda)} \; ; \; r = \sum_{(i,\lambda)\in C} e_i^{(\lambda 1)}(e_i^{(1\lambda)}\varphi) . \tag{42}$$

It follows from (27) and (28) that

$$r' e_j^{(\mu\nu)} r = (e_j^{(\mu 1)}\varphi)e_j^{(1\nu)} r = (e_j^{(\mu 1)}\varphi)e_j^{(11)}(e_j^{(1\nu)}\varphi) .$$

Since $e_j^{(11)} = e_j^{(11)}\varphi$ by (41), this yields

$$r' e_j^{(\mu\nu)} r = e_j^{(\mu\nu)}\varphi. \tag{43}$$

If we take $\mu = \nu$, add over all j and μ, and use (31), we find $r'r = 1$. Similarly, we have

$$rr' = \sum_{i,\lambda} e_i^{(\lambda 1)}(e_i^{(11)}\varphi)e_i^{(1\lambda)} = \sum_{i,\lambda} e_i^{(\lambda 1)} e_i^{(11)} e_i^{(1\lambda)} = \sum_{i,\lambda} e_i^{(\lambda)} = 1 .$$

Thus, r' is the reciprocal r^{-1} of r. By (43) the inner automorphism

J(r) maps $e_j^{(\lambda\mu)} \longrightarrow e_j^{(\lambda\mu)}\varphi$ for all j, λ, μ. Moreover, if $s \in S^{\#}$, then $1_0 s 1_0 = s$. By (42) and (32),

$$r^{-1}sr = r' 1_0 s 1_0 r = \sum_{i=0}^{k} (e_i^{(11)}\varphi)e_i^{(1)} s \sum_{j=0}^{k} e_j^{(1)} e_j^{(11)}\varphi .$$

Since $e_i^{(11)} = e_i^{(1)}$ and $e_i^{(1)}\varphi = e_i^{(1)}$, we find $r^{-1}sr = 1_0 s 1_0 = s$.

It is now clear that $J(r)\varphi^{-1}$ leaves fixed all $s \in S^{\#}$ and all $e_j^{(\lambda\mu)}$. Since $M^{\#}$ is generated by $S^{\#}$ and the set $\{e_j^{(\lambda\mu)}\}$, (p.182), $J(r)\varphi^{-1}$ is the identity. Hence φ is the inner automorphism J(r) and the proof is finished.

8. Further results and corollaries.

DEFINITION 3. Let R be a ring with unit element. Then R is *primary*, if R/Rad (R) is simple and R is *completely primary*, if R/Rad (R) is a skew field.

In other words, the completely primary rings are the reduced rings with a unit element which have height 1 . Since a Cartesian sum of $k \geqq 2$ skew fields is not simple, the completely primary rings can also be defined as the *reduced primary rings*. It follows from (J*) that an m-ring R with unit element 1 is completely primary iff the module $R^{\cdot}$ is indecomposable, and this is equivalent with saying that 1 is the only idempotent.

A ring R with unit element is primary, iff there does not exist an ideal H with $\mathrm{Rad}(R) \subset H \subset R$. It follows from (M) and (I) that an m-ring R and its reduced ring have the same height and are primary at the same time. Hence the primary m-rings are exactly the m-rings with unit element which have height 1.

(S) A primary m-ring R is isomorphic with a complete matrix ring S_q over a completely primary m-ring S. Conversely, for such an S, the rings S_q are primary m-rings.

Proof: Since R has a unit element, we can apply (A). Here, S has height 1 and it is a completely primary ring. Its unit element e is the only idempotent. The checkered matrix ring $M(S, \{e\}, \{q\})$ consists of all matrices of degree q_1 with coefficients in $eSe = S$. Hence R is isomorphic with S_q (with $q = q_1$).

Conversely, if S is a completely primary m-ring, (M) and (N) imply that S_q is an m-ring of height 1. Since S has a unit element, S_q is primary.

It follows from (I) that an m-ring R and its reduced ring S are semisimple at the same time. If S here has height k, S is a direct sum of K ideals T_j which are skew fields; $S = \oplus \sum_{j=1}^{k} T_j$. Now (I) shows that R is a direct sum $R = \oplus \sum_{j=1}^{k} H_j$ of k ideals H_j. Each H_j is a simple ring since an ideal H with $0 \subset H \subset H_j$ would be an ideal of R and hence would correspond to an ideal L of S with $0 \subset L \subset T_j$ which is impossible. This is Wedderburn's first theorem. Since S has clearly a unit element, so has R. Wedderburn's second theorem is the special case of (S) dealing with a simple R.

Let R be an arbitrary m-ring of height k. As in Section 2, let

$e_1, e_2, \ldots, e_k$ be k indecomposable idempotents of R such that e_iR and e_jR are not R-isomorphic for $i \neq j$. It follows from (H) that the k rings

$$P_1 = e_1Re_1 \ , \ P_2 = e_2Re_2 , \ldots , P_k = e_kRe_k$$

are completely primary. We call these rings the k completely primary rings associated with R. It is seen easily (e.g. from (C4)) that if e_i is replaced by an idempotent $e^*_i \in R$ such that e_iR and e^*_iR are R-isomorphic, then $e^*_iRe^*_i$ and e_iRe_i are ring isomorphic. Using (Q), we see that the k rings P_i are determined by R apart from isomorphisms. If $e_1, \ldots, e_k$ are chosen as in Section 2, and the notation is the same, $e_i 1_0 = 1_0 e_i = e_i$ and hence $P_i = e_i 1_0 R 1_0 e_i = e_iSe_i$. Hence

(T) An m-ring R and its reduced ring S have the same associated completely primary rings.

If R is an m-ring, we may identify R with the isomorphic checkered matrix ring $M = M(S, \{e\}, \{q\})$ obtained in Section 2. Let N denote the set of matrices $[m_{\tau\omega}] \in M$ whose coefficients $m_{\tau\omega}$ belong to Rad (R). It follows from Section 2 that N = Rad (R).

For $j = 1, 2, \ldots, k$, let C_j be the set $\{(j, \mu)\}$ with $1 \leqq \mu \leqq q_j$. Denote by B_j the set of elements

$$\sum_{\tau, \omega \in C} \tilde{m}_{\tau\omega}$$

with $m_{\tau\omega} \in e_\tau Re_\omega = e_jRe_j = P_j$. Then B_j is the set of matrices $[m_{\tau\omega}]$ which have coefficients different from zero only in the q_j rows and columns belonging to pairs $(j, \mu) \in C_j$, $1 \leqq \mu \leqq q_j$. The coefficients in these q_j

rows and columns can be arbitrary elements of P_j. It is now clear that B_j is isomorphic with the complete matrix ring $(P_j)_{q_j}$ of degree q_j over P_j. Furthermore, if $B = \sum_{j=1}^{k} B_j$, each B_j is an ideal of the ring B and the sum is direct.

Finally, let A be the set of all sums $\sum \tilde{m}_{\tau\omega}$ with $\tau = (i, \lambda)$, $\omega = (j, \mu)$ such that either $i \neq j$ or $i = j = 0$. Clearly, A is an additive subgroup and $R = A \dot{+} B$. Moreover, by (18) $e_\tau R e_\omega \subseteq \text{Rad}(R)$ in our present case. Hence $A \subseteq \text{Rad}(R)$, and we have the following result (essentially due to Wedderburn):

(U) If R is an m-ring of height k, R can be written as a direct sum $R = A \dot{+} B$ such that A is an additive subgroup of the radical and that B is isomorphic with a Cartesian sum $\oplus \sum_{j=1}^{k} B_j$ of k primary rings, $B_j \approx (P_j)_{q_j}$. Here, $P_1, P_2, \ldots, P_k$ are the k completely primary rings associated with R.

We readily obtain the corollary

(U*) If the notation is as in (U), then

$$R/\text{Rad}(R) \approx \oplus \sum_{j=1}^{k} (T_j)_{q_j}$$

where T_j is the skew field $T_j = P_j/\text{Rad}(P_j) = P_j/(P_j \cap \text{Rad}(R))$.

We give a further definition which will become important later in connection with Wedderburn's "third" theorem.

DEFINITION 4: A ring R is cleft, if R can be written as a direct sum $R = G \dot{+} \text{Rad}(R)$ where G is a subring of R, necessarily isomorphic with $R/\text{Rad}(R)$.

We prove here only the following proposition which will be applied later :

(V) Let R be an m-ring. If the completely primary rings $P_1, P_2, \ldots, P_k$ associated with R are cleft, then R is cleft.

Proof: As in the proof of (U), we may identify R with a checkered matrix ring M. Assume that each P_j is cleft, say $P_j = L_j \dot{+} Q_j$ where L_j is a subring and $Q_j = \text{Rad}(P_j) = P_j \cap \text{Rad}(R)$. Let N have the same significance as in the proof of (U). It follows from (18) that $\tilde{m}_{\tau\omega} \in N$ except when τ and ω belong to the same set C_j; $1 \leqq j \leqq k$. If $\tau, \omega \in C_j$ and $m_{\tau\omega} \in e_j R e_j = P_j$, we can write $m_{\tau\omega} = x_{\tau\omega} + y_{\tau\omega}$ with $x_{\tau\omega} \in L_j$ and $y_{\tau\omega} \in Q_j \subseteq \text{Rad}(R)$. Then $\tilde{m}_{\tau\omega} = \tilde{x}_{\tau\omega} + \tilde{y}_{\tau\omega}$ and $\tilde{y}_{\tau\omega} \in N$. Let G be the set of all elements of the form

$$g = \sum_{j=1}^{k} \sum_{\tau,\omega \in C_j} \tilde{x}_{\tau\omega}$$

with $x_{\tau\omega} \in L_j$. It follows easily from (26) that G is a subring of M and that $M = G + N$. Moreover, $G \cap N = (0)$, the sum is direct and $R = M$ is cleft.

The converse of (V) holds too, see Problem 11.

Problems to Chapter VI

DEFENITION. If ρ is an element of a ring R, we say that ρ has characteristic 0, if $n\rho = \rho + \rho + \ldots + \rho$ (n terms) is different from 0 for every natural integer n. If there exist natural integers n for which $n\rho = 0$, the characteristic of ρ is the smallest such n. If R has a unit element 1, the characteristic of 1 is called the characteristic of R.

Note that if $\rho = \alpha\beta$ with $\alpha, \beta \in R$, the characteristic of ρ divides that of α and β. If R has a unit element, the characteristic of every ρ divides the characteristic of R. The characteristic of a skew field is either 0 or a prime number p.

1. Let X be an r-ideal of a ring R. Show that an idempotent e of the ring X is indecomposable, iff e is indecomposable as an idempotent of the ring R.

2. Let R be a reduced ring of height k which has a unit element $\mathbf{1}$; $R/\mathrm{Rad}(R) \approx \oplus \sum_{j=1}^{k} T_j$ where T_j are skew fields. Assume that each T_j has characteristic 0. Show that $\mathbf{1}$ cannot be written as a sum of more than k idempotents (not necessarily orthogonal).

3. Suppose that R is a ring with a unit element such that the total number h of idempotents in R is finite.

(a) Show that h is odd.

(b) Show that if R is an m-ring and $h = 3$, then R is isomorphic with a Cartesian sum of two completely primary rings.

(c) Show that if R is an m-ring, then $R/\mathrm{Rad}(R)$ is isomorphic with a Cartesian sum of simple rings which either have a finite number of elements or are skew fields.

4. Let R be a ring with a unit element, let η be an idempotent and set $P = \eta R \eta$.

(a) If X ranges over the r-ideals of P and if $Y = XR$, show that $X \longrightarrow Y$ is a multiplicative isomorphism of the set $\{X\}$ of r-ideals of P into the set of r-ideals of R.

(b) If there does not exist an ideal H of R with $\eta \in H \subset R$, show that $X \longrightarrow Y$ maps $\{X\}$ onto the set of r-ideals Y of R with $Y \subseteq \eta R$.

(c) If $N = \mathrm{Rad}(R)$ show that $N \cap P \subseteq \mathrm{Rad}(P)$.

(d) If R is either an m-ring or the extended ring $R_0^{\#}$ belonging to an m-ring R_0, show that $N \cap P = \mathrm{Rad}(P)$.

5. Let R be an m-ring with unit element, let η be an idempotent, and set $P = \eta R \eta$.

(a) If R is quasi-uniserial, so is P.

(b) If R is uniserial, so is P.

(c) Give an example of an m-ring R with a unit element such that all associated completely primary rings are uniserial, but R is not quasi-uniserial.

6. Let R be an m-ring with unit element, and let S be its reduced ring. Show that R is quasi-uniserial iff S is quasi-uniserial. Show that R is uniserial, iff S is uniserial.

7. Let R be a completely primary m-ring with unit element 1 .

(a) Show that the characteristic of R is either 0 or a power p^m of a prime number p ; $m \geqq 1$.

(b) Show that there exist subfields K of the center of R with the unit element 1, iff the characteristic of R is either 0 or a prime number p.

8. Define a semiprimary ring R as a ring R which possesses a nilpotent ideal N such that R/N is a semisimple m-ring. Show that the results of Chapter VI remain valid, if the class of m-rings is replaced by the class of semiprimary rings.

Note that in the proof of Theorem A, it suffices to assume that N is a nilideal. Of course, we can then only show that Rad (S) is a nilideal and not that it is nilpotent. In order to have all the results of Chapter VI, one may also consider the class of all rings R with a "locally nilpotent" ideal N such that R/N is a semisimple m-ring. Here an ideal N is said to be locally nilpotent, if every finite set of elements of N belongs to a nilpotent ideal.

Hint: Use Problem 27 of Chapter IV.

9. Let R = $M(S, \{e\}, \{q\})$ be a checkered matrix ring with unit element, S a reduced m-ring. Find the center of R.

10. Let R be an m-ring with unit element, of height k. Show that the center of R is isomorphic with a Cartesian sum of k rings C_i such that $C_i / \mathrm{Rad}\,(C_i)$ is a field, $(i = 1, 2, \ldots, k)$.

11. Let R be an m-ring. Prove the converse of (V): If R is cleft, each completely primary ring P associated with R is cleft. Deduce that R is cleft, iff its reduced ring S is cleft.

APPENDIX A

1. Groups with operators.

We assume a knowledge of the definition of groups and of their elementary properties. Most frequently, the group operation will be written as addition. Thus, if G is a group and if $a, b \in G$, we have a sum $a + b \in G$ and this addition is associative. There exists a neutral element or zero element 0 such that $a + 0 = 0 + a = a$ for all $a \in G$. For every $a \in G$, there exists an inverse element $-a \in G$ such that $a + (-a) = (-a) + a = 0$.

Let K be an arbitrary set of elements (possibly empty). We say that G is a group with K as set of operators or more briefly that G is a K-group, if for all $g \in G$ and all $\alpha \in K$, the product $g\alpha$ is defined as an element of G such that

$$(1) \qquad (g + h)\alpha = g\alpha + h\alpha$$

for all $g, h \in G$ and all $\alpha \in K$. In other words, for each $\alpha \in K$, the mapping $g \longrightarrow g\alpha$ is a homomorphism of G into G. This implies that $0\alpha = 0$, $(-g)\alpha = -(g\alpha)$.

If G is a K-group, a K-subgroup H is a subset which is itself a K-group, if the same operations as for G are used. Then, H has to satisfy the following conditions: 1) If h and $h_1 \in H$, then $h + h_1 \in H$. 2) If $h \in H$, then $-h \in H$. 3) If $h \in H$ and $\alpha \in K$, then $h\alpha \in H$. Conversely, these three conditions guarantee that H is a K-subgroup.

Remarks: 1. Instead of K-subgroup, one also says "admissible subgroup". If it is quite clear that we are dealing with operator groups, we may sometimes use the term "subgroup" to mean "K-subgroup".

2. If $g_1, g_2 \in G$, we often write $g_1 - g_2$ for $g_1 + (-g_2)$, in particular when G is abelian. The conditions 1) and 2) for subgroups H can then be replaced by the one condition: If $h_1, h_2 \in H$, then $h_1 - h_2 \in H$.

3. Occasionally, other notations are used for the product $g\alpha$ of an element $g \in G$ with an element $\alpha \in K$. For instance, we may find it convenient to write αg or g^{α} for $g\alpha$.

Let H be a K-subgroup of G. If g and g' are elements of G, we say that g and g' are (left) congruent (mod H) if g' has the form $g' = h + g$ with $h \in H$, that is, if $g' + (-g) \in H$. We sometimes write then $g' \equiv g \pmod{H}$. Clearly, congruence is an equivalence relation. The residue class or coset $\lfloor g \rfloor = \lfloor g \rfloor_H$ of g is the set of all elements of G congruence to g; $\lfloor g \rfloor = \{h+g \mid h \in H\}$. Clearly, $\lfloor g \rfloor = \lfloor g' \rfloor$, iff $g \equiv g' \pmod{H}$.

A K-subgroup H of G is normal, if $(-g) + h + g \in H$ for all $g \in G$ and $h \in H$. If H is a normal K-subgroup of G, congruences mod H can be added: If $g_1 \equiv g'_1$ and $g_2 \equiv g'_2 \pmod{H}$, then $g_1 + g_2 \equiv g'_1 + g'_2 \pmod{H}$. This implies that an addition of the residue classes can be defined by the formula

(2) $$\lfloor g_1 \rfloor + \lfloor g_2 \rfloor = \lfloor g_1 + g_2 \rfloor$$

Moreover, since $g \equiv g'$ (mod H) implies $g\alpha \equiv g'\alpha$ mod H for every $\alpha \in K$, a multiplication of the residue classes with the operaotrs $\alpha \in K$ can be defined by

(3) $$\lfloor g \rfloor \alpha = \lfloor g\alpha \rfloor .$$

It is seen readily that the set of all residue classes modulo a fixed normal K-subgroup K forms a K-group with those operations. This is the quotient group or residue class group G/H. The zero element is the residue class $\lfloor 0 \rfloor$ of the zero element of G. Clearly, $\lfloor 0 \rfloor = H$. Moreover, $\lfloor -g \rfloor = -\lfloor g \rfloor$.

We shall have to deal mainly with abelian K-groups. Here , of course, every K-subgroup is normal.

2. Sums of normal K-subgroups.

Let G be a K-group and let $\{H_j\}$ be a family of normal K-subgroups where j ranges over a set J of indices . Let S denote the set of all elements g of G which can be written as sums $g = \sum_i x_i$ of finitely many elements x_i each of which belongs to some H_j. It is seen easily that S then is a normal K-subgroup of G. We call S the sum $S = \sum_{j \in J} H_j$ of the H_j. Note that this addition of subgroups is commutative, because of the normality of the H_j. It is also associative.

We now discuss the notion of a direct sum. First of all, we require that every element of H_i commutes with every element of H_j for $i, j \in J$, $i \neq j$. Then every element s of S can be written in the form

$$(4) \qquad s = \sum_{j \in J} h_j$$

with $h_j \in H_j$. Here, the understanding is that only finitely many h_j are different from 0 so that the sum in (4) is really only a finite sum, even if J is an infinite set. Because of our first assumption concerning the $\{H_i\}$, the order in which the h_i in (4) are taken will not matter.

Secondly, we require now that for each $s \in S$, the representation (4) of s is unique. If both our conditions are satisfied, we call the sum of $\{H_i\}$ direct and we indicate this by placing a dot in front of the summation sign and writing $S = \bullet\sum_j H_j$. (If we have finitely many groups H_i and use $+$ signs, a dot is placed above each $+$.)

The following remarks are more or less obvious.

(I) It suffices to check the second requirement for the element $s = 0$. We have to show here that (4) for $s = 0$ implies that all h_i are 0.

(II) The second requirement can be replaced by the following condition: For each $j \in J$, the intersection

$$H_j \cap \sum_{i \neq j} H_i = (0).$$

(III) It follows from (II) that we must have $H_i \cap H_j = (0)$ for $i, j \in J$, $i \neq j$. Actually, this condition implies that the first requirement is satisfied.

Indeed, suppose that $x \in H_i$, $y \in H_j$. Since H_i and H_j both are normal in G, the commutator element $\gamma = (-x) + (-y) + x + y$ belongs to both H_i and H_j. If $H_i \cap H_j = (0)$, we have $\gamma = 0$ and this yields $x + y = y + x$.

(IV) In particular, the sum $H_1 + H_2$ of two normal K-subgroups is direct, iff $H_1 \cap H_2 = (0)$.

(V) A sum $\sum_{j \in J} H_j$ of a family $\{H_j\}$ of normal K-subgroups of G is direct, iff the sum $\sum_{j \in F} H_j$ is direct for every finite subset F of J.

Indeed, if $\sum_{j \in J} H_j$ is direct, obviously $\sum_{j \in F} H_j$ is direct for every subset F of J. Conversely, suppose that $\sum_{j \in F} H_j$ is direct for every finite subset of J. If $i, j \in J$, $i \neq j$, take $f = \{i, j\}$. Then $H_i + H_j$ is direct and hence every $x \in H_i$ commutes with every $y \in H_j$. If we had a non-trivial representation (4) of $s = 0$, there exists a finite subset F of J consisting of the subscripts j of the terms $h_j \neq 0$ in (4). Then $\sum_{j \in F} H_j$ would not be direct.

(VI) If $S = \bullet\sum_{j \in J} H_j$ is direct and if H_j is written as a direct sum $\bullet\sum_{r \in L_j} H_{j,r}$ of a family $\{H_{j,r}\}$ of normal K-subgroups of G, then S is the direct sum of the $H_{j,r}$ for all pairs (j, r).

We are interested almost exclusively in abelian K-groups. Here of course every K-subgroup is normal and our first requrement for direct sums is always satisfied.

3. Operator homomorphisms.

Let G and G* be two K-groups, both with the same set K of operators. A K-homomorphism or operator homomorphism of G into G* is a mapping θ of G into G* with the following two properties:

(I) If $g \longrightarrow g^*$ and $g_1 \longrightarrow g_1^*$, then $g + g_1 \longrightarrow g^* + g^*_1$.

(II) If $g \longrightarrow g^*$, then $g\alpha \longrightarrow g^*\alpha$ for every $\alpha \in K$. If the image of g is denoted by $g\theta$, this can be expressed by the equations

$$(5) \qquad (g + g_1)\theta = g\theta + g_1\theta, \; (g\alpha)\theta = (g\theta)\alpha,$$

for all $g, g_1 \in G$ and $\alpha \in K$. Note that 0θ is the zero element of G^* and that $(-g)\theta = -(g\theta)$.

We say of course that G is mapped onto G^*, if every element of G^* is image of an element of G or, symbolically, if $G\theta = G^*$. If the mapping is one-to-one, we speak of an R-isomorphism. If it is absolutely clear that we are dealing with K-groups, we may sometimes omit the "prefix" K before homomorphism. On the other hand, if we wish to emphasize that the condition (II) holds for θ, we say that θ "admits" the operator α.

As an example of a K-homomorphism, we mention the natural K-homomorphism of a group G onto a quotient group G/H (where H is a normal K-subgroup of G). This is the mapping which maps every element g on the residue class $\lfloor g \rfloor$ containing g.

Let θ be a K-homomorphism mapping the K-group G onto the K-group G^*. The kernel H is the subset of G mapped on the zero-element 0^* of G^*. It is seen easily that H is a normal K-subgroup of G. Moreover, there exists a well-defined mapping $\tilde{\theta}$ of G/H onto G^* such that $\lfloor g \rfloor\tilde{\theta} = g\theta$. (i.e., if θ maps $g \longrightarrow g^*$, then $\tilde{\theta}$ maps $\lfloor g \rfloor \longrightarrow g^*$). It is now clear that $\tilde{\theta}$ is a K-isomorphism of G/H onto G^*. Using the symbol $\approx$ for K-isomorphism, we have

$$G/(\text{Kernel } \theta) \approx G^* . \tag{6}$$

The preceding statements, in particular (6), represent the "First Theorem on homomorphic groups".

If the notation is as before and if A is a K-subgroup of G, its image $A\theta$ is certainly a K-subgroup B of G^*. However, different subgroups of G may be mapped onto the same B(e.g., the subgroup (0) and the kernel H are both mapped on (0^*). For each K-subgroup B of B^*, there exists a K-subgroup A of G mapped onto B. We only have to take for A the reciprocal image $B\theta^{-1}$ of B, i.e., the set of all elements of G whose image belongs to B. If A is chosen as $B\theta^{-1}$, then $A \supseteq H$ and it is now clear that A is the only K-subgroup $\supseteq H$ of G mapped onto B. This gives the first part of the following "Second Theorem on homomorphic groups"

1) If θ is a K-homomorphism of the K-group G onto the K-group G^* with the kernel H, there exists a one-to-one correspondence $A \longrightarrow B$ between the set $\{A\}$ of all K-subgroups $A \supseteq H$ of G and the set $\{B\}$ of all K-subgroups B of G^* such that

$$B = A\theta , \quad A = B\theta^{-1} ; \tag{7}$$

2) If $A \in \{A\}$ is normal in G, then $B = A\theta$ is normal in G^* and conversely. In this case,

$$G/A \approx G^*/B. \tag{8}$$

The first statement 2) is obvious. In order to prove (8), consider more generally a normal K-subgroup R of G and a normal K-subgroup S of G* such that $R\theta \subseteq S$. If we map $\underline{g|}_R \longrightarrow \underline{g\theta|}_S$, we clearly obtain a K-homomorphism $\tilde{\theta}$ of G/R onto G*/S. This is the homomorphism $\tilde{\theta}$ of G/R onto G*/S induced by θ. If $S = B$, $R = A = B\theta^{-1}$, $\tilde{\theta}$ is an isomorphism and (8) holds.

A K-subgroup G is simple, if $G \neq (0)$ and if the only normal K-subgroups are the trivial ones, (0) and (G). A normal K-subgroup A of G is maximal normal, if $A \neq G$ and if there does not exist a normal K-subgroup A_1 with $A \subset A_1 \subset G$. Applying the "Second Theorem" to the natural homomorphism of G onto G/H (with the kernel H), we have the important corollary:

Corollary: A normal K-subgroup H of the K-group is maximal normal in the K-group G, iff G/H is simple.

Third Theorem on homomorphic groups. Let U and V be two normal K-subgroups of the K-group G. Then

$$(U + V)/U \approx V/(U \cap V) , \tag{9}$$

where each denominator is a normal K-subgroup of the corresponding numerator .

Proof: Let θ be the natural homomorphism of G onto G/U and let η be the restriction $\theta | V$ of θ to V . Thus, η is the mapping $v \longrightarrow \underline{v|}_U$ of V. If $g \in U + V$, we can write $g = u + v$ with $u \in U$, $v \in V$. Hence $\underline{g|}_U = \underline{v|}_U$. It is now clear that η is a K-homomorphism of V onto (U + V)/U. We have $v \in \text{Kernel } (\eta)$, iff $v \in U$, i.e., iff $v \in U \cap V$. Application of the first theorem on homomorphic groups to η yields (9).

The following definition is not very important for us (but very important in other connection): Consider a sequence of K-groups $\{G_r\}$ and K-homomorphisms φ_r of G_r into G_{r+1},

$\longrightarrow G_r \xrightarrow{\varphi_r} G_{r+1} \xrightarrow{\varphi_{r+1}} G_{r+2} \longrightarrow \ldots$. Here, r is to range over all integers with $a < r < b$, (a finite or $-\infty$, b finite or $+\infty$). We say that the sequence is exact, if $G_r\varphi_r \subseteq \text{Kernel}(\varphi_{r+1})$ for $a < r$, $r + 2 < b$.

4. Composition series.

Let G be a K-group and let A and B be two K-subgroups with $A \supseteq B$. A composition series from A to B is a finite sequence $H_0, H_1, \ldots, H_m$ of subgroups such that

(I) $H_0 = A \supset H_1 \supset \ldots \supset H_m = B$.

(II) Each H_i is a maximal normal K-subgroup of H_{i-1}, $1 \leqq i \leqq m$.

As shown by the corollary in Section 3, (II) can be replaced by the condition that H_i is a normal K-subgroup of H_{i-1} and that H_{i-1}/H_i is simple. The number m is called the length of the composition series.

A composition series of G is simply a composition series from $A = G$ to $B = (0)$. If such composition series of G exist, the length of the shortest composition series of G is called the Jordan dimension d(G) of G. If no composition series of G exist, set $d(G) = \infty$. Note that $d(G) = 0$, if $G = (0)$ and that $d(G) = 1$, if G is simple.

(A) Let G be a K-group and N a normal K-subgroup. There exist composition series from G to N, iff $d(G/N) < \infty$.

Proof: Suppose that

(10) $$H_0 = G \supset H_1 \supset H_2 \supset \dots \supset H_m = N$$

is a composition series from G to N. Let θ be the natural homomorphism of G onto G/N and let θ_j be its restriction to H_j. Set $H^*_j = H_j\theta = H_j\theta_j$. Since H_{j+1} is a maximal normal subgroup of H_j, the second theorem on homomorphic groups (applied to θ_j) shows that H^*_{j+1} is a maximal normal subgroup of H^*_j. Hence

(11) $$H^*_0 = G/N \supset H^*_1 \supset H^*_2 \supset \dots \supset H^*_m = (0^*)$$

is a composition series of G/N.

Conversely, if we start from a composition series (11) of G/N and set $H_j = H^*_j\theta^{-1}$, the second theorem on homomorphic groups shows that (10) is a composition series from G to N.

We say that a composition series $\{H_j\}$ goes through a group L if L is one of the groups H_j.

(B) Let G be a K-group and N a normal K-subgroup. There exist composition series of G through N, iff both $d(G/N)$ and $d(N)$ are finite.

Proof: If we have a composition series of G through N, the part from N to (0) is a composition series of N. On the other hand, the part from G to N can be used to obtain a composition series of G/N, cf. (A).

Conversely, if we have a composition series of G/N, then (A) furnishes a composition series from G to N. If we also have a composition series of N, we simply have to put this behind the composition series from G to N. This yields a composition series of G through N.

(C̲) Let G be a K-group of finite dimension d(G) and let N be a normal K-subgroup. There exist composition series of G through N.

Proof: We use induction on $n = d(G)$. For $n = 0$, $G = (0)$ and (C) is trivial. Assume $n > 0$ and let

$$H_0 = G \supset H_1 \supset \dots \supset H_n = (0)$$

be a composition series of length n. Then $H_1 \supset H_2 \supset \dots \supset H_n = (0)$ is a composition series of length $n - 1$ of H_1. Hence, (C̲) holds for H_1 instead of G.

In $N \subseteq H_1$, we can find a composition series of H_1 through N. Placing a term G in front of this composition series, we obtain a composition series of G through N.

We may then assume $N \not\subseteq H_1$. Clearly, $H_1 + N$ is a normal K-subgroup of G and $H_1 + N \supset H_1$. Since H_1 was maximal normal, we must have $H_1 + N = G$. Set $H_1 \cap N = T$. Applying the third theorem on homomorphic groups twice, we find

$$G/H_1 \approx N/T \ , \tag{12}$$

$$G/N \approx H_1/T \ , \tag{13}$$

where each denominator is normal in the corresponding numerator. In particular, T is normal in H_1 and since (C̲) holds for H_1, it follows from (B̲) that $d(H_1/T) < \infty$, $d(T) < \infty$. By (13), $d(G/N) < \infty$. On the other hand, since G/H_1 is simple, $d(G/H_1) = 1$ and hence

$d(N/T) = 1$ by (12). Since $d(N/T) < \infty$, $d(T) < \infty$, we have $d(N) < \infty$ by (B) and as $d(G/N) < \infty$, (B) shows that there exist composition series of G through N.

If $H_0 = G \supset H_1 \supset \dots \supset H_n = (0)$ is a composition series, we call the n simple groups

$$H_0/H_1, H_1/H_2, \dots, H_{n-1}/H_n$$

the quotient groups of the composition series. If $L_0 = G \supset L_1 \supset \dots \supset L_n = (0)$ is a second composition series of the same length, we say that both composition series have isomorphic quotient groups, if there exists a permutation $i \longrightarrow i^*$ of $\{1, 2, \dots, n\}$ such that

$$H_{i-1}/H_i \approx L_{i^*-1}/L_{i^*} \qquad (\text{for } 1 \leqq i \leqq n).$$

(D) Theorem of Jordan Hoelder: If G is a K-group and $d(G) < \infty$, then every composition series of G has length $d(G)$ and any two composition series have isomorphic quotient groups.

Proof: 1) We use again induction on $n = d(G)$; the case $n = 0$ is trivial. Let

$$H_0 = G \supset H_1 \supset \dots \supset H_n = (0) \tag{14}$$

be a composition series of length $n = d(G)$ and let

$$L_0 = G \supset L_1 \supset \dots \supset L_m = (0) \tag{15}$$

be a second composition series of G.

As in the proof of (C), $d(H_1) = n - 1$ and hence (D) holds for H_1 instead of G. If $H_1 = L_1$, then $H_1 \supset H_2 \supset \dots$ and $H_1 = L_1 \supset L_2 \supset \dots$ are two composition series of H_1. Applying (D) here we see at once that $n = m$ and that (14) and (15) have isomorphic quotient groups.

2) Assume then $H_1 \neq L_1$. Set $N = L_1$. Since L_1 was maximal normal, it follows that $L_1 \not\subseteq H_1$. If we set $T = H_1 \cap N$, again (12) and (13) hold. It follows from ($\underline{C}$) that there exist composition series $T \supset T_1 \supset \ldots$ of T. Now form

$$G \supset H_1 \supset T \supset T_1 \supset \ldots , \tag{16}$$

$$G \supset N = L_1 \supset T \supset T_1 \supset \ldots . \tag{17}$$

We claim that these are two composition series of G. Indeed the only question in (16) is whether T is maximal normal in H_1. However, this is immediate from (13) since $G/N = G/L_1$ is simple. Similarly, (12) shows that T is maximal normal in N and that (17) is a composition series. Both series (16) and (17) have the same length. Moreover, (12) and (13) show that they have isomorphic quotient groups. Indeed starting with T/T_1, the quotient groups are the same and $G/H_1 \approx L_1/T$, $H_1/T \approx G/L_1$.

Compare now the composition series (14) and (16). Since they have the same second term H_1, the argument in 1) shows that they have the same length n and isomorphic quotient groups. It follows that (14) and (17) too have the same length n and isomorphic quotient groups.

Finally compare (17) and (15). Since they have the same second term L_1 and since (17) has the length $n = d(G)$, again the argument in 1) applies. Both series have the same length and isomorphic quotient

quotient groups.

(E) If G is a K-group and N a normal K-subgroup

$$d(G) = d(G/N) + d(N) . \qquad (18)$$

(Here the sum is taken as ∞, if a summand is ∞.)

Indeed, if $d(G) < \infty$, we can find a composition series through N. The proof of (A) shows that the length of the piece from G to N is $d(G/N)$. Now (18) states that the length of the composition series of G is equal to the sum of the lengths of the pieces from G to N and from N to (0).

On the other hand, if $d(G) = \infty$, (B) shows that at least one of $d(G/N)$, $d(N)$ is ∞.

5. The chain conditions.

Let G be a set and let U be a family of subsets of G. If $S \in U$ we shall say that S is a U-set. In particular, we are interested in the cases that G is a K-group and that U consists of the normal K-subgroups of G.

If $\mathfrak{X}$ is a subfamily of U, a *minimal member* of $\mathfrak{X}$ is an element S of $\mathfrak{X}$ such that no proper subset S_1 of S belongs to $\mathfrak{X}$. Similarly, $S \in \mathfrak{X}$ is a *maximal member* of $\mathfrak{X}$, if no subset $S_1 \supset S$ of G belongs to $\mathfrak{X}$. We say that G satisfies the *minimum condition* (m-condition) for U-sets, if every non-empty family $\mathfrak{X}$ of U-sets has minimal members. Similarly, G satisfies the *maximum condition* (M-condition) for U sets, if every non-empty family $\mathfrak{X}$ of U-sets has maximal members. The set G satisfies the descending chain condition (d. c. c.) for U-sets if in every "descending" sequence

$$X_1 \supseteq X_2 \supseteq X_3 \supseteq \dots$$

of U-sets, only finitely many X_n are distinct, that is, if there exists an index n_0 such that $X_n = X_{n+1}$ for $n \geq n_0$. Finally, G satisfies the ascending chain condition (a. c. c.) for U-sets, if in every ascending sequence

$$X_1 \subseteq X_2 \subseteq X_3 \subseteq \dots$$

of U-sets, only finitely many X_n are distinct.

The following remark is trivial.

(F) The m-condition for U-sets is equivalent with the d. c. c., the M-condition with the a. c. c.

Indeed, if the m-condition holds, any descending sequence $\{X_n\}$ has minimal member X_{n_0} and then $X_{n_0} = X_{n_0+1} = X_{n_0+2} = \dots$. On the other hand, if $\mathfrak{X}$ is a family of U-sets without minimal members, then we can use induction to define a set $X_n \in \mathfrak{X}$ for $n = 1, 2, \dots,$ such that $X_n \supset X_{n+1}$. Hence the d. c. c. does not hold. The proof for the M-condition is similar.

Suppose that U satisfies the following two conditions:

(I) $G \in U$; the empty set $\emptyset$ is not in U.

(II) Every intersection of U-sets belongs to U.

For every subset S of G, we can form the intersection $\overline{S}$ of all U-sets $T \supseteq S$. Clearly, $\overline{S}$ is a U-set, $\overline{S} \supseteq S$, and $\overline{S}$ is a subset of every U-set $T \supseteq S$. We call $\overline{S}$ the U-set generated by S and we often denote this set by (S). The set S is a U-set, iff $S = (S)$. We say that a U-set X is finitely generated, if there exists a finite subset S of G with $(S) = X$.

(G). If the a.c.c. holds for U-sets, then every U-set is finitely generated.

Proof: Suppose that X is a U-set which is not finitely generated. Then $X \neq \emptyset$. If S is a finite subset of X, certainly $(S) \neq X$. Since $S \subseteq X$ and X is a U-set, $(S) \subset X$ and there exist elements $x \in X$ with $x \notin (S)$. Starting from an arbitrary element s_1 of X we can use induction to construct a sequence $\{s_n\}$ of elements of X such that if S_n is the set $\{s_1, s_2, \ldots, s_n\}$, we have

$$(S_1) \subset (S_2) \subset (S_3) \ldots .$$

This shows that the a.c.c. does not hold for U-sets.

(G*) If U in addition to (I) and (II) satisfies the further condition that the union of an ascending sequence $\{X_n\}$ of U-sets is a U-set, the converse of (G) holds: If every U-set is finitely generated, the a.c.c. holds for U-sets.

Indeed, if $\{X_n\}$ is an ascending chain of U-sets, it is assumed that $S = \bigcup_n X_n$ is a U-set and then that it is finitely generated. Since all "generators" must belong to some X_n, we have $S = X_n$.

We return to the discussion of K-groups.

(H) If G is a K-group which has a composition series, the a.c.c. and the d.c.c. hold for normal K-subgroups of G. For abelian K-groups, G, the converse is true: If both chain conditions hold, G has a composition series.

Proof: Suppose that $d(G) < \infty$. It follows from (E) that if X and Y are normal K-subgroups of G and $X \subset Y$ then $d(X) < d(Y)$. If $\{X_n\}$ is an ascending sequence of normal K-subgroups of G then $d(X_n) \leqq d(G)$ and our remark shows that we can have only finitely many distinct X_n. The proof of the d.c.c. is similar.

Suppose now that G is abelian and assume the a.c.c. (M-condition) for K-subgroups of G. If $H \neq (0)$ is a K-subgroup and if we take for $\mathfrak{X}$ the family of all proper subgroups of H, we see that there exist maximal (proper) K-subgroups of H. Apply this first to $H = G$, then to a maximal (proper) K-subgroup H of G and so on. Suppose that G has no composition series. Then all groups remain different from (0). By induction, we can define a descending sequence $\{H_n\}$ for all n such that H_n is a maximal (proper) K-subgroup of H_{n-1}. This is impossible, if we assume the d.c.c.

For non-abelian K-groups G, it can be shown that G has a composition series, iff both chain conditions hold for "semi-normal" K-subgroups. It is not necessary for our purposes to discuss this concept.

(I) Suppose that a K-group G is written as sum of a finite number of normal K-subgroups H_i,

$$G = \sum_{i=1}^{n} H_i$$

If the m-conditions hold for the normal K-subgroups of each H_i, the same is true for G. An analogous rule holds for the M-condition.

Proof: 1) Set $L_r = \sum_{i=1}^{r} H_i$ for $1 \leqq r \leqq n$, $L_0 = (0)$. Let X be a normal K-subgroup of G. For each r with $1 \leqq r \leqq n$, set

$$(19) \qquad T_r(X) = H_r \cap (L_{r-1} + X).$$

Then $T_r(X)$ is a normal K-subgroup of H_r.

(2) Let $Y \subseteq X$ be a normal K-subgroup of G. Clearly, $T_r(Y) \subseteq T_r(X)$ for $1 \leqq r \leqq n$. Assume that here the equality sign holds for all r. We wish to show next that then

$$(20) \qquad X \subseteq L_r + Y, \qquad \text{for } 0 \leqq r \leqq n.$$

This is certainly true for $r = n$, since $L_n = G$. Assume that (20) has been proved for some $r \geqq 1$. Now, $L_r = L_{r-1} + H_r$. If $x \in X$, it follows from (20) that we may set $x = \ell_{r-1} + h_r + y$ with $\ell_{r-1} \in L_{r-1}$, $h_r \in H_r$, $y \in Y$. Since $x, y, \ell_{r-1} \in L_{r-1} + X$, we have $h_r \in L_{r-1} + X$ and, by (19) $h_r \in T_r(X)$. By assumption, $T_r(X) = T_r(Y)$ and hence $h_r \in T_r(Y) \subseteq L_{r-1} + Y$. Hence $x = \ell_{r-1} + h_r + y \in L_{r-1} + Y$. This shows that (20) holds for $r - 1$ instead of r.

Thus, (20) holds for all $r \geqq 0$. For $r = 0$, we obtain $X \subseteq Y$, that is, $X = Y$.

Thus, if Y is a K-subgroup of X and $T_r(X) = T_r(Y)$ for all r, then $X = Y$.

3) Consider now a descending chain of normal K-subgroups

$$X_1 \supseteq X_2 \supseteq X_3 \supseteq \cdots .$$

Then, for each r with $1 \leqq r \leqq n$,

$$T_r(X_1) \supseteq T_r(X_2) \supseteq T_r(X_3) \supseteq \cdots .$$

Since the descending chain condition holds for normal K-subgroups of H_r, we may determine an index m_0 such that

$$T_r(X)_m = T_r(X_{m+1}) \tag{21}$$

for $m \geqq m_0$. Here, m_0 may be taken the same for all r since we have only finitely many r. Then (21) holds for $m \geqq m_0$ for all r. As shown in 2), this implies $X_m = X_{m+1}$, for $m \geqq m_0$. Thus, the descending chain condition holds for normal K-subgroups of G.

4) The proof in the case of the M-condition is quite analogous to that in 3).

6. Completely reducible groups.

A K-group G is completely reducible or semisimple if G is the sum of normal simple K-subgroups F_j

$$G = \sum_{j \in J} F_j . \tag{22}$$

The following two theorems will be proved simultaneously.

(J) Every completely reducible K-group G is a direct sum of normal simple K-subgroups.

(K) If G is a completely reducible K-group and H is a normal K-subgroup, both H and G/H are completely reducible. Moreover, there exists a normal K-subgroup H_1 such that $G = H \dotplus H_1$.

Proof: Let H be a normal K-subgroup of the completely reducible K-group G. Suppose that S is a set of normal simple K-subgroups F_j for which (22) holds. Consider subsets T of S such that both $\sum_{F_j \in T} F_j$ and $H + (\sum_{F_j \in T} F_j)$ are direct. Let $\mathfrak{X}$ be the family of all subsets T of S with this property. Since the empty set $T = \emptyset$ has the property required of sets T , $\emptyset \in \mathfrak{X}$, and $\mathfrak{X}$ is not empty.

We now apply Zorn's lemma (Section 10) in a standard fashion. We order $\mathfrak{X}$ by inclusion. Let $\mathcal{L}$ be a linearly ordered subfamily of $\mathfrak{X}$ and let T* denote the union $T^* = \bigcup_{T \in \mathcal{L}} T$. (Each $T \in \mathcal{L}$ is a set of subgroups $F_i \in S$ and so is T*; we have $F_i \in T^*$, if $F_i \in T$ for some T in $\mathcal{L}$.)

It is easily seen that $T^* \in \mathfrak{X}$. Indeed, on account of the remark (V) in Section 2 , it suffices to prove that the sum

$$(23) \qquad H + F_{i_1} + F_{i_2} + \dots + F_{i_n}$$

is direct for any finite subset $\{F_{i_1}, F_{i_2}, \dots, F_{i_n}\}$ of T*. Here, each F_{i_ν} belongs to some $T \in \mathcal{L}$ and since $\mathcal{L}$ is linearly ordered and we have only finitely many F_{i_ν} , there exist $T_0 \in \mathcal{L}$ such that

$F_{i_1}, F_{i_2}, \ldots, F_{i_n}$ all belong to T_0. Since T_0 here is an element of $\mathcal{X}$, the sum (23) really is direct.

Thus, $T^* \in \mathcal{X}$. Clearly, $T \subseteq T^*$, for all $T \in \mathcal{L}$. Hence, $\mathcal{L}$ has an upper bound in $\mathcal{X}$ and Zorn's lemma applies. It follows that there exist maximal elements T of $\mathcal{X}$. Set

$$G_0 = H \dot{+} \left(\cdot\sum_{F_i \in T} F_i \right), \tag{24}$$

where we know that the sums are direct. Here, G_0 is a normal K-subgroup of G.

We wish to show that $G_0 = G$. If this was not so it would follow from (22) that there exist $F_j \in S$ with $F_j \not\subseteq G_0$. This implies $F_j \cap G_0 \subset F_j$ and since $F_j \cap G_0$ is a normal K-subgroup of G and F_j is simple, $F_j \cap G_0 = (0)$. Now the remark (IV) in Section 2 shows that $G_0 + F_j$ is direct. But it then follows easily that if we form a set T_1 by adding the one element F_j to the set T (i.e., $T_1 = T \cup \{F_j\}$), then the sum

$$G_0 \dot{+} F_j = H \dot{+} \left(\cdot\sum_{F_i \in T_i} F_i \right)$$

is direct. This means that $T_1 \in \mathcal{X}$ and since $T \subset T_1$, T would not be maximal in $\mathcal{X}$, a contradiction. This proves that $G_0 = G$.

Taking now $H = (0)$, the equation (24) yields $(\underline{J})$. Moreover, for an arbitrary normal K-subgroup H, the last part of $(\underline{K})$ is obtained from (24) by setting

$$H_1 = \dot{\sum_{F_i \in T}} F_i \quad . \tag{25}$$

Then $G/H \approx H_1$ and (25) shows that G/H is completely reducible. Since we now know that every quotient group of G is completely reducible, this applies to $G/H_1 = (H \dot{+} H_1)/H_1 \approx H$ and (K) is proved in all parts.

(L) If G is a completely reducible K-group, the minimum and the maximum condition for normal K-subgroups of G imply each other.

Proof: 1) Assume the ascending chain condition. If

$$X_1 \supseteq X_2 \supseteq X_3 \ldots$$

is a descending chain of normal K-subgroups, it follows from (J) that there exist normal K-subgroups Z_n of G with $G = X_n \dot{+} Z_n$ and normal K-subgroups Y_n of X_n with $X_n = X_{n+1} \dot{+} Y_n$. Since every element of Z_n commutes with every element of $Y_n \subseteq X_n$, the group Y_n is normal in $G = X_n \dot{+} Z_n$. Then

$$X_1 = X_2 \dot{+} Y_1 = X_3 \dot{+} Y_2 \dot{+} Y_1 = X_4 \dot{+} Y_3 \dot{+} Y_2 \dot{+} Y_1 = \ldots \quad .$$

If we set $Y^*_n = \sum_{i=1}^{n} Y_i$, this sum is direct and Y^*_n is a normal K-subgroup. Since $Y^*_n \subseteq Y^*_{n+1}$, the ascending chain condition shows that there exists an n_0 such that $Y^*_{n-1} = Y^*_n$ for $n \geq n_0$. This implies $Y_n = (0)$, whence $X_n = X_{n+1}$ for $n \geq n_0$. Hence the descending chain condition holds.

2) Assume the descending chain condition. Suppose that

$$X_1 \subseteq X_2 \subseteq X_3 \subseteq \cdots$$

is an ascending chain of normal K-subgroups of G. Without restriction, we may take $X_1 = (0)$. We wish to define a descending chain $\{Y_n\}$ of normal K-subgroups of G such that

$$G = X_n \dot{+} Y_n \qquad (n = 1, 2, 3, \ldots). \tag{26}$$

For $n = 1$, we may take $Y_1 = G$. If $Y_1, Y_2, \ldots, Y_n$ have already been found, it follows from (J) that we can find a nomal K-subgroup Y_{n+1} of Y_n such that

$$Y_n = (X_{n+1} \cap Y_n) \dot{+} Y_{n+1}. \tag{27}$$

It follows from (26) that Y_{n+1} is normal in G. Since the sum (27) is direct, $X_{n+1} \cap Y_n \cap Y_{n+1} = (0)$ and as $Y_{n+1} \subseteq Y_n$, this implies

$$X_{n+1} \cap Y_{n+1} = (0). \tag{28}$$

Substituting (27) in (26) and using $X_n \subseteq X_{n+1}$, we find $G = X_{n+1} + Y_{n+1}$. By (28), this sum is direct and it follows that (26) holds for $n + 1$ with $Y_n \supseteq Y_{n+1}$.

This shows then that we can define a descending chain $\{Y_n\}$ such that (26) holds for all n. Because of the chain condition, there exists an n_0 such that $Y_n = Y_{n+1}$ for $n \geq n_0$, and then $G = X_n \dot{+} Y_n = X_{n+1} \dot{+} Y_n$. Since $X_n \subseteq X_{n+1}$, this implies $X_{n+1} = X_n$ for $n \geq n_0$. Hence the ascending chain condition holds.

7. Cartesian products and sums of K-groups.

Let $\{G_\nu\}$ be a family of K-groups all with the domain K of operators. Assume first that we have finitely many G_ν, say that ν ranges over the set $J = \{1, 2, \dots, n\}$ of indices. Then the set theoretical of Cartesian product $P = \prod_\nu G_\nu$ is the set of all n-tuples.

$$p = (g_1, g_2, \dots, g_n), \tag{29}$$

with $g_\nu \in G$ for $\nu \in J$. If $p' = (g'_1, \dots, g'_n)$ is a second element of P and if $\alpha \in K$, we define operations in P by

$$p + p' = (g_1 + g'_1, \dots, g_n + g'_n), \quad p\alpha = (g_1\alpha, \dots, g_n\alpha).$$

Then p becomes a K-group, the Cartesian direct product $\boxed{\times}_\nu G_\nu$.

This definition can be extended to the case that we have infinitely many G_ν. Let J again denote the set of indices. Instead of (29), we take mappings g of J which associate an element $g_\nu \in G_\nu$ with each $\nu \in J$. (These are special mappings of J into the union $\bigcup_\nu G_\nu$.) If we define the sum of two such mappings and the product $g\alpha$ for $\alpha \in K$ in the usual manner, we obtain again a K-group $P = \boxed{\times}_\nu G_\nu$ the Cartesian direct product. If we take only the elements $g \in P$ such that g_ν is the zero element 0_ν of G_ν for all but a finite number of indices $\nu \in J$, we obtain a K-subgroup S of P. This is the Cartesian direct sum $S = \oplus \sum_\nu G_\nu$ of the G_ν. Of course, if J is a finite set, $S = P$. We are mainly interested in S.

For each $\mu \in J$, we have a K-isomorphism i_μ of G_μ into S (and hence into P) which maps the element $x \in G_\mu$ on the element $g \in S$ with $g_\mu = x$ and $g_\nu = 0$ for $\nu \in J$, $\nu \neq \mu$. This is the

μ-th injection i_μ. On the other hand, we have a K-homomorphism p_μ of $S = \oplus\sum_\nu G_\nu$ onto G_μ where p_μ maps the element $g \in S$ on its value g_μ for the argument $\mu \in J$. This is the μ-th projection p_μ. It is seen at once that

(30) $$i_\mu p_\mu = I_\mu \text{ , } i_\mu p_\nu = \square_{\mu\nu} \quad \text{for } \mu \neq \nu .$$

Here, I_μ is the identity map of G_μ and $\square_{\mu\nu}$ the map which maps every element of G_μ on 0_ν. On the other hand,

(31) $$\sum_{\nu \in J} p_\nu i_\nu = I \text{ ,}$$

the identity map of S; for each $x \in S$, only a finite number of terms $xp_\nu i_\nu$ are $\neq 0$.

The μ-th injection i_μ maps G_μ onto the K-subgroup $\overline{G}_\mu$ of S. It is seen easily that $\overline{G}_\mu$ is a normal K-subgroup of S, that the elements of $\overline{G}_\mu$ commute with the elements of $\overline{G}$ for $\mu \neq \nu$, and then that S is the direct sum of $\overline{G}_\nu$,

(32) $$\oplus\sum_{\nu \in J} G_\nu = \bullet\sum_{\nu \in J} \overline{G}_\nu .$$

Here, of course, G_ν and $\overline{G}_\nu$ are K-isomorphic.

Conversely, suppose that a K-group G is a direct sum $G = \bullet\sum_{\nu \in J} G_\nu$ of normal K-subgroups G_ν of G. As in (4), every element $s \in G$ has a unique representation

$$s = \sum_{\nu \in J} h_\nu$$

with $h_\nu \in G_\nu$ such that h_ν is the zero element of G_ν except for a finite number of indices $\nu \in J$. Let g be a function defined on J such that $g(\nu) = h_\nu$ for every $\nu \in J$. It is seen readily that $g \in \oplus\sum_\nu G_\nu$

and that the mapping s ⟶ g is a K-isomorphism of $\bullet\sum_{\nu \in J} G_\nu$ onto $\oplus\sum_{\nu \in J} G_\nu$. Thus

$$(33) \qquad \bullet\sum_{\nu \in J} G_\nu \approx \oplus\sum_{\nu \in J} G_\nu \quad .$$

Because of (32) and (33), we usually consider a direct sum $\bullet\sum G_\nu$ as more or less the same thing as the Cartesian sum $\oplus\sum_\nu G_\nu$. For instance, we identify in (32) the given group G_ν with the K-isomorphic group $\bar{G}_\nu$.

8. Fitting's Lemma.

A K-group $G \neq (0)$ is said to be indecomposable, if G cannot be written as a direct sum of normal K-subgroups $\neq (0)$, G of G. We prove *Fitting's Lemma* :

(*M*) Let G be an indecomposable K-group of finite Jordan dimension d(G). Let θ be a K-endomorphism of G which maps normal K-subgroups of G onto normal K-subgroups of G. Then either θ is a K-automorphism of G or θ is nilpotent (i.e., some power θ^n is the zero-mapping $\square$)*.

Proof: 1) Set $G_0 = G$, $G_n = G\theta^n$ for n = 1, 2, ..., Since θ maps normal subgroups of G onto normal subgroups, and since $G_1 = G\theta \subseteq G_0$, we see successively that all G_n are normal K-subgroups of G and that

$$(34) \qquad G_0 = G \supseteq G_1 \supseteq \dots \supseteq G_n \supseteq \dots \quad .$$

On the other hand, let H_n be the kernel of θ^n. Then H_n is a normal K-subgroup of G. If $x \in H_n$, we have $x\theta^n = 0$ whence $x\theta^{n+1} = 0$, that is, $x \in H_{n+1}$. Thus,

---

* A *K-endomorphism* of G is a K-homomorphism of G into G. A *K-automorphism* of G is a K-isomorphism of G onto G.

(35) $$H_0 = (0) \subseteq H_1 \subseteq H_2 \ldots \subseteq H_n \subseteq \ldots .$$

Now, by (H) both chain conditions hold hold for normal K-subgroups of G. Consequently, $G_n = G_{n+1} = G_{n+2} = \ldots$ and $H_n = H_{n+1} = H_{n+2} = \ldots$ for all sufficiently large n. If we choose such an n, we have $G_n = G_{2n}$, $H_n = H_{2n}$. Set $X = G_n = G\theta^n$ and $Y = H_n$. Then $X\theta^n = G\theta^{2n} = G_{2n} = X$. Hence

(36) $$G\theta^n = X = X\theta^n , \quad H_n = H_{2n} = Y .$$

Let g be an element. Since $g\theta^n \in X = X\theta^n$, we may find elements $x \in X$ with $g\theta^n = x\theta^n$. Then $g - x$ belongs to the kernel $H_n = Y$ of θ^n. This implies that $G = X + Y$. We claim that this sum is direct. Indeed, if $d \in X \cap Y$, then by (36) $d \in X\theta^n$ and we can set $d = x_0\theta^n$ with $x_0 \in X$. Since d belongs to the kernel $Y = H_n$ of θ^n, here $0 = d\theta^n = x_0\theta^{2n}$. Thus x_0 belongs to the kernel H_{2n} of θ^{2n}. However, then by (36) $x_0 \in H_n$ and $x_0\theta^n = 0$. It follows that $d = 0$, $X \cap Y = (0)$.

Hence $G = X \dot{+} Y$ is a direct sum. Since G was indecomposable, either $X = (0)$ or $Y = (0)$. In the former case, $G\theta^n = (0)$, that is, $\theta^n = \square$ and θ is nilpotent.

Suppose then that we have the second case $Y = (0)$ whence $G = X$, that is, $G_n = G$ and $H_n = (0)$. It follows from (34) and (35) that $G_1 = G$ and $H_1 = (0)$. Thus, θ maps G onto $G_1 = G$. Since its kernel H_1 is (0), θ is a K-automorphism of G.

9. The Krull -Schmidt Theorem.

It will be sufficient for our purposes to deal with the case of abelian K-groups. We prove first a simple remark.

($\underline{N}$) Let $G \neq (0)$ be an abelian K-group such that the m-condition holds for K-subgroups of G. Then G can be written as a direct sum of finitely many indecomposable K-subgroups.

Proof: Let $\mathcal{X}$ be the family of all K-subgroups $\neq (0)$ which cannot be written as direct sum of finitely many indecomposable K-subgroups. If $\mathcal{X}$ is not empty, it has minimal members H. Since H cannot be written as direct sum of indecomposable K-groups, H must be decomposable; say $H = A \dot{+} B$ where A and B are K-subgroups $\neq (0)$. Then $A \subset H$ and $B \subset H$. Since H is minimal in $\mathcal{X}$, $A \notin \mathcal{X}$, $B \notin \mathcal{X}$. Hence A and B can be written as direct sums of finitely many indecomposable K-groups. But then the same would be true for $H = A \dot{+} B$; we have a contradiction.

It follows that $\mathcal{X}$ is empty. In particular, $G \notin \mathcal{X}$ and this yields ($\underline{N}$).

Our problem is to study the uniqueness of the summands of the decomposition in ($\underline{N}$).

We use the following notation. If φ is a mapping of a set S and if T is a subset of S, $\varphi | T$ denotes the restriction of φ to T. The identity map of S is denoted by I_S. If a K-group G is written as a direct sum $G = A \dot{+} B$, we denote the projection of G onto A by $p(A \dot{+} B \longrightarrow A)$ or simply p_A. Thus, p_A maps $a + b \longrightarrow a$ for $a \in A$, $b \in B$. (If several decompositions occur, we may indicate by superscripts which of them is used in projection.)

LEMMA 1_0. Let G be a K-group and suppose that

$$G = A \dot{+} B = C \dot{+} D ,$$

where A, B, C, D are K-subgroups of G. Set $p_B^{(1)} = p(A \dot{+} B \longrightarrow B)$. Then $p_B^{(1)} | D$ has the kernel $A \cap D$. Moreover $p_B^{(1)} | D$ maps D onto B, iff $A + D = G$.

Proof: Since $p_B^{(1)}$ has the kernel A, $p_B^{(1)} | D$ has the kernel $A \cap D$. If $d \in D$ and if $d = a + b$ with $a \in A$, $b \in B$, then $p_B^{(1)} | D$ maps $d \longrightarrow b = d - a$. Hence the image of D under $p_B^{(1)} | D$ is $B \cap (A + D)$. This image is B, iff $B \subseteq A + D$. Since $A \subseteq A + D$, this is so iff $G = A + B \subseteq A + D$; that is, iff $G = A + D$.

LEMMA 1. Let A, B, C, D be as in Lemma 1_0. Set again $p_B^{(1)} = p(A \dot{+} B \longrightarrow B)$ and set $p_C^{(2)} = p(C \dot{+} D \longrightarrow C)$. Then $p_B^{(1)} | D$ is a K-isomorphism of D onto B, iff $p_C^{(2)} | A$ is a K-isomorphism of A onto C.

Indeed, by Lemma 1_0, $p_B^{(1)} | D$ is a K-isomorphism of D onto B, iff $A \cap D = (0)$, $A + D = G$. Interchanging A and D, B and C in Lemma 1_0, we see that $p_C^{(2)} | A$ is a K-isomorphism of A onto C, iff the same conditions $A \cap D = (0)$, $A + D = G$ hold.

Definition 1. Let φ be a K-homomorphism of the K-group A into the K-group C. Then φ is invertible with respect to C, if there exists a K-homomorphism ψ of C into A such that

(37) $$\varphi\psi = I_A .$$

LEMMA 2. If φ is a K-homomorphism of the K-group $A \neq (0)$ into the indecomposable K-group C and if φ is invertible with respect to C, then φ is a K-isomorphism of A onto C.

Proof: Suppose that $\varphi\psi = I_A$ as in (37). Then φ must have kernel (0). Let $M \subseteq C$ be the kernel of ψ. If $x \in C$, then $x\psi \in A$ and hence $x\psi = x\,\psi\varphi\psi$. Thus $(x - x\psi\varphi)\psi = 0$, that is, $x - x\psi\varphi \in M$. It follows that $C = A\varphi + M$. If $a\varphi \in A\varphi \cap M$ with $a \in A$, then $a\varphi\psi = 0$, and by (37), $a = 0$. Hence $A\varphi \cap M = (0)$, the sum $C = A\varphi \dot{+} M$ is direct.

But C was indecomposable. Since $A \neq (0)$ and φ is an isomorphism, $A\varphi \neq (0)$. Hence $M = 0$, that is, $A\varphi = C$ and we are finished.

Definition 2: An indecomposable abelian K-group A is a Fitting group, if every K-endomorphism of A is either an automorphism or nilpotent.

LEMMA 3: Let A be a Fitting group and let φ be a K-homomorphism of A into the abelian K-group C which is invertible with respect to C. Suppose that C is written as a direct sum $C = C_1 \dot{+} C_2$ of K-groups and set $p_i = p(C_1 \dot{+} C_2 \longrightarrow C_i)$, $i = 1, 2$. If $i = 1$ or 2 is taken suitably, φp_i is invertible with respect to C_i.

Proof: Clearly, $p_1 + p_2 = I_C$. Let ψ be a K-homomorphism of C into A such that $\varphi\psi = I_A$ whence $\varphi(p_1 + p_2)\psi = I_A$. If we set $\theta_i = \varphi p_i \psi$ for $i = 1, 2$, we have

(38) $$\theta_1 + \theta_2 = I_A .$$

We use the fact that the K-endomorphisms of A form a ring E with the unit element I_A. Both θ_1 and θ_2 are elements of E. Since $\theta_2 = I_A - \theta_1$, θ_1 and θ_2 commute. If we raise (38) to some exponent h it follows that I_A is a sum of terms $\theta_1^a \theta_2^b$ with $a + b = h$. Then $a \geqq h/2$ or $b \geqq h/2$. If θ_1 and θ_2 were both nilpotent, we could choose h so large that for each of our terms $\theta_1^a \theta_2^b$, we have $\theta_1^a = \square$ or $\theta_2^b = \square$. This would give the absurd equation $I_A = \square$.

Thus, at least one θ_i is not nilpotent. Since A was a Fitting group, then θ_i is a K-automorphism of A and hence θ_i has an inverse θ_i^{-1} in E. It follows that $I_A = \theta_i \theta_i^{-1} = \varphi p_i \psi \theta_i^{-1}$. If $\psi_i = (\psi \theta_i^{-1}) | C_i$, then ψ_i is a K-homomorphism of C_i into A. Since φp_i maps A into C_i, we find $\varphi p_i \psi_i = I_A$ and φp_i is invertible with respect to C_i.

We now come to the proof of the uniqueness theorem which we state in the form

(Q) Let G be an abelian K-group which is written in two ways as direct sum of indecomposable K-groups.

(39) $$G = \bullet \sum_{\mu=0}^{m} G_\mu = \bullet \sum_{\nu=0}^{n} H_\nu .$$

Assume that each G_μ with $\mu > 0$ is a Fitting group. Then $m = n$ and if the H_μ are taken in suitable order, $G_\mu \approx H_\mu$ for $\mu = 0, 1, \ldots, m$.

Proof: If $m = 0$, $G = G_0$ is indecomposable and we must have

$n = 0$, $G = H_0$ and ($\underline{Q}$) holds. We use induction with respect to m. Suppose that $m > 0$ and set $A = G_m$, $B = \sum_{\mu=0}^{\cdot m-1} G_\mu$. Consider all K-subgroups C which satisfy the following two conditions (a) and (b).

(a) C is a sum $\sum_{\nu \in N} H_\nu$ with ν ranging over a non-empty subset N of $\{0, 1, \ldots, n\}$. If Q is the complementary subset of $\{0, 1, 2, \ldots, n\}$, set $D = \sum_{\nu \in Q}^{\cdot} H_\nu$ so that $G = C \dot{+} D$.

(b); If $p_C = p(C \dot{+} D \longrightarrow C)$, then $\varphi = p_C | A$ is invertible with respect to C.

Such groups C exist. For instance, $C = G$ has the required properties. Here, $D = (0)$, $p_C = I_G$, and $\varphi = I_A$. Then the projection $\psi = p(A \dot{+} B \longrightarrow A)$ is a K-homomorphism of G into A and $\varphi\psi = I_A$.

Choose a group $C = \sum_{\nu \in N} H_\nu$ with the properties (a) and (b) such that N is a subset of $\{0, 1, \ldots, n\}$ with the smallest possible number of elements. If the H_ν are arranged suitably, we may assume that $n \in N$. If N contains other indices, we can write $C = C_1 \dot{+} C_2$ where $C_1 = H_n$ and $C_2 \neq (0)$ is a sum of groups H_ν. It follows easily from Lemma 3 that either C_1 or C_2 has also properties (a) and (b). This is inconsistent with our choice of C. Hence $N = \{n\}$, $C = H_n$, $D = \sum_{\nu=0}^{\cdot n-1} H_\nu$.

We have $G = A \dot{+} B = C \dot{+} D$. Since $\varphi = p_C | A$ is invertible with respect to C and since $C = H_n$, Lemma 2 shows that $p_C | A$ is a K-isomorphism of A onto C. Now Lemma 1 applies (with $p_C = p_C^{(2)}$). It follows that $\chi = p_B^{(1)} | D$ is a K-isomorphism of D onto B. Hence

$$\cdot\sum_{\mu=0}^{m-1} G_\mu = B = D\chi = \cdot\sum_{\nu=0}^{n-1} (H_\nu\chi) .$$

This is a formula of the same type as (39) with m replaced by m - 1 . Consequently, Theorem (Q) may be applied here. It follows that $m - 1 = n - 1$ and that for a suitable arrangement of the H_ν, we have $G_\mu \approx H_\mu\chi$ for $\mu = 0, 1, \ldots, m-1$. Thus , $m = n$, $G_\mu \approx H_\mu$ and as $p_C|A$ is a K-isomorphism of $A = G_n$ onto $C = H_m = H_n$, this holds also for $\mu = n$. This shows that (Q) holds for (39).

Note that our proof does not require that G_0 is a Fitting group. This is important in Chapter VII. Actually, in the application made there of (Q) , it is clear that the groups G_μ with $\mu > 0$ are Fitting groups, independent of Fitting's Lemma.

If we assume that d(G) if finite, every indecomposable direct summand A of G has finite dimension and is a Fitting group by (M). Combining (N) and (Q) , we have the *Krull-Schmidt Theorem* , at least for abelian K-groups.

(Q*) Theorem: Let G be an (abelian) K-group which has a composition series. Then G can be written as a direct sum of indecomposable K-groups and these summands are determined apart from K-isomorphism.

The same method can be used in the non-abelian case, but some additional remarks become necessary.

10. Remarks on Zorn's Lemma.

Let S be a set. Suppose that a binary relation ρ is defined for the elements of S and that we write $a < b$, iff the relation holds true for the ordered pair $< a , b >$ of elements of S. We say that ρ defines a partial order in S, if the following conditions hold (for $a, b, c \in S$);

(a) The statements $a < b$, $a = b$, $b < a$ are mutually exclusive.

(b) If $a < b$ and $b < c$, then $a < c$.

We have a linear order, if in (a) always exactly one of the statements $a < b$, $a = b$, $b < a$ holds.

If ρ defines a partial order in S and if T is a subset of S, then ρ also defines an order in T. If T then is linearly ordered, we call T a chain of S. An element s of S is called an upper bound of the chain T, if $t \leqq s$ for every $t \in T$.

Zorn's Lemma: Suppose that S is a partially ordered set and that every chain of S has an upper bound in S. Then there exist maximal elements m of S, i.e., elements $m \in S$ such that there does not exist an element x of S with $m < x$.

Zorn's Lemma can be proved from the axioms of set theory. It is equivalent with the axiom of choice (assuming of course all the other axioms).

In many applications, S is a set consisting of subsets of a given set M. If $x, y \in S$ and if we define $x < y$ to mean $x \subset y$ (that is, that x is a proper subset of y), we have a partial order in S. We say then that we have ordered S by inclusion. If T is a chain and if we choose u_T as the union of T (i.e., as the set of all elements of M which belong to some $t \in T$), then $t \leqq u_T$ for every $t \in T$. If S has the property that the union of each chain T of S belongs to S, T has an upper bound in S and Zorn's Lemma applies.

[illegible]-5-68

QA
247
B7
pt.1

Brauer, Richard
Non-commutative rings

Physical &
Applied Sci.

PLEASE DO NOT REMOVE
CARDS OR SLIPS FROM THIS POCKET

UNIVERSITY OF TORONTO LIBRARY